Facultad
de
Ciencias

Números de Carmichael

Carmichael numbers

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Pablo González Mazón
Director: Daniel Sadornil Renedo

Junio 2019

Agradecimientos

La persona que más se merece el agradecimiento por este trabajo es Daniel Sadornil. Gracias por haberte preocupado por mí, por el buen trato que siempre me has dado sin merecerlo, por haber escuchado mis diatribas y por haber procurado que consiga lo mejor de mí mismo. Dudo que otra persona se hubiera volcado en este trabajo de la manera en que tú lo has hecho. Aunque quizás tú no lo veas así, creo que nuestra relación es especial. Gracias por haber sido mi profesor, mi director de trabajo de fin de grado, y antes que lo anterior, gracias por ser mi amigo.

También quiero dar gracias a los profesores de la Facultad de Ciencias por su gran labor docente, en especial a aquellos que me han ayudado este último año. Por su puesto, agradezco a todos mis amigos, dentro y fuera de clase, el seguir aguantándome. Marta, me traes un poco loco.

Por último, doy gracias a mi padre y a mi madre por todo lo que hoy tengo, a mi hermano por haberme eneseñado a pensar (aunque sigo haciéndolo peor que tú, yo soy más de imaginar) y a mi abuela, a quien dedico este trabajo. Gracias al resto de mi familia por cuidar de mí.

Resumen

Este trabajo pretende ser una guía para que el lector se introduzca en el estudio de los números de Carmichael. Se comienza introduciendo varias nociones que conducen, de forma natural, a la definición de esta familia de números. Posteriormente, se estudian algunas de sus propiedades más elementales y algunos procedimientos para generarlos. El texto termina discutiendo resultados concernientes a la distribución de los números de Carmichael. A lo largo del trabajo, se discuten algunas de las conjeturas y problemas abiertos relacionadas con estos números, así como posibles líneas de investigación. Como un objetivo secundario, este trabajo busca que el lector interesado pueda familiarizarse con técnicas y resultados al uso en el estudio de la teoría de números.

Palabras clave: pequeño teorema de Fermat, pseudoprimo, número de Carmichael, forma universal, función contador de números de Carmichael C.

Abstract

This work aims to be a guide for the reader to introduce to the study of Carmichael numbers. Firstly, we introduce several concepts that lead to a natural definition of this family of numbers. Later on, we study some of the most relevant properties regarding these numbers, as well as some procedures to generate them. The text ends with the discussion of results concerning the distribution of Carmichael numbers. Throughout this document, some of the conjectures and open problems related to these numbers are brought up. As a secondary objective, this work allows the interested reader to become familiar with some habitual techniques and results to be used in number theory.

Key words: Fermat's little theorem, pseudoprime, Carmichael number, universal form, Carmichael number counting function C.

"La vida es demasiado corta para no pensar en matemáticas."

Pablo González Mazón[1]

[1]Es posible que otros lo haya dicho antes, pero no lo he encontrado referenciado en ninguna parte.

Índice general

Capítulo 1

Introducción

Una de las familias de números más sencillas de entender es el anillo de enteros $(\mathbb{Z}, +, \cdot)$. Prácticamente todos, incluso aquellos no familiarizados con la labor matemática, comprenden las "reglas de juego" a través de las que los anteriores pueden manipularse. Lo que hace que estos números tan elementales sigan siendo un área de estudio es la dificultad intrínseca a algunas de las definiciones que las personas inventamos. Consideremos el siguiente ejercicio,

$$\textit{Sea } n \in \mathbb{N},\ n \geq 3.\ \textit{Demostrar que } A = \{(a,b,c) \in \mathbb{Z}^3 : a^n + b^n = c^n\} = \varnothing\ .$$

Aunque el problema anterior ha sido motivo de estudio desde 1637, el primero en resolverlo fue Andrew Wiles [Wil95], lo que le valió el Premio Abel en 2016. Es sensato preguntarse si merece la pena dedicar tiempo y esfuerzo a demostrar enunciados como el anterior, ya que si bien el resultado es interesante puede que su utilidad no sea proporcional a su dificultad. El verdadero valor del problema anterior fue la cantidad de ideas nuevas y teorías matemáticas que florecieron durante la búsqueda de una demostración: se dieron los primeros pasos hacia la teoría de anillos, se comprobó que determinados dominios admitían más de una factorización en irreducibles y se definieron los dominios de factorización única, se introdujo la noción de ideal (de la mano de Dedekind), y por supuesto las matemáticas desarrolladas por Wiles en [Wil95] son un auténtico logro. Podría decirse que el fin último de la teoría de números es el de generar nuevas matemáticas, susceptibles de aplicarse en otros contextos.

Una de las definiciones más fructíferas en relación a los números enteros es la noción de número primo. Son verdaderamente muchos los resultados relacionados con los números primos, y algunos de los problemas más importantes del momento están directamente relacionados con ellos: ¿FACTORING $\in \mathcal{P}$?¿Es cierta la hipótesis de Riemann? En este trabajo, nos centramos en el estudio de una de las ideas que surge de uno de los primeros, y más importantes, resultados sobre los números primos: el pequeño teorema de Fermat. Como veremos en el Capítulo 1, el pequeño teorema aporta una condición necesaria para que un número sea primo. Adelantando acontecimientos, la condición que se impone para que n sea primo es

$$a^n \equiv a \pmod{n}\ , \tag{1.1}$$

para cualquier base a. El interés en la búsqueda de números primos motivó la pregunta sobre si esta condición era suficiente para garantizar que n es primo. Así lo creyeron por algún tiempo los matemáticos chinos, quienes escribieron que todo entero n satisfaciendo $2^{n-1} \equiv 1$ debía ser primo. La falsedad de este resultado, conocido como "Probléme Chinois", fue demostrada por Alwin Korselt. Sin embargo, el estudio de los números satisfaciendo (1.1) motivó la definición de pseudoprimo de Fermat, que también introducimos

en el siguiente capítulo. De nuevo, en afán de hacer del pequeño teorema de Fermat un test de primalidad, cabe preguntarse si el siguiente enunciado (que no es más que el recíproco del pequeño teorema) es cierto,

$$\textit{Si } a^n \equiv a \pmod{n} \textit{ para cualquier entero } a\textit{, entonces } n \textit{ es primo.}$$

El enunciado anterior es el punto de partida de este trabajo. Como comprobaremos, se trata de una afirmación falsa. La demostración de esto último pasa por la búsqueda de algún número de Carmichael. Los números de Carmichael se definen como los números compuestos que satisfacen la hipótesis del enunciado anterior (aunque nosotros los definimos de un modo ligeramente distinto, que como demostraremos es equivalente).

Este trabajo es una primera introducción al estudio, tanto algebraico como analítico, de los números de Carmichael. En el Capítulo 1 comenzamos introduciendo, de forma natural y con rigor, toda la matemática previa que conduce a los números de Carmichael. Concluiremos el mismo demostrando la existencia de los números de Carmichael. Seguiremos analizando algunas de sus propiedades más importantes en el Capítulo 2, y veremos diferentes formas de caracterizarlos. Dado que uno de los aspectos de mayor interés en este contexto es precisamente la construcción de números de Carmichael, dedicamos el Capítulo 3 a desarrollar algunas técnicas útiles. Finalmente, en el Capítulo 4 estudiaremos el conjunto de los números de Carmichael en el contexto de la teoría analítica de números, centrándonos en su distribución.

A lo largo de nuestro estudio, veremos cómo los números de Carmichael están relacionados con otros teoremas importantes en teoría de números, así como con algunas conjeturas. Volviendo a la idea inicial de esta introducción, aunque como el último teorema de Fermat puede que los números de Carmichael no tengan grandes aplicaciones, es muy probable que muchas de las ideas que emanan de su estudio den lugar a nuevos trabajos, teorías, o con suerte, a aplicaciones útiles.

Capítulo 2

El pequeño teorema de Fermat y su recíproco

Uno de los resultados mejor conocidos en teoría de números es el "pequeño" teorema de Fermat, aportado por el matemático francés Pierre de Fermat [Fle91] en el siglo XVII. Su importancia reside en las múltiples aplicaciones que tiene dentro distintos contextos de las matemáticas. En primer lugar, muchos tests de primalidad surgen a partir del pequeño teorema. Como ejemplo de ello encontramos los tests de Rabin-Miller y AKS. Por otra parte, se trata de un teorema habitual en el estudio de cuerpos finitos. Los primeros ejemplos estos últimos son de la forma $\mathbb{F}_p$, con p un número primo, y es bien sabido que todo elemento de éstos anula al polinomio $X^p - X$. Así mismo, muchos sistemas criptográficos se apoyan en este resultado, y aunque otros como el RSA se fundamenten en el teorema de Eüler, éste no deja de ser una generalización del pequeño teorema. Finalmente, es un teorema íntimamente relacionado con el grupo de unidades de los anillos $(\mathbb{Z}/n\mathbb{Z})$. De acuerdo con el teorema de estructura de grupos abelianos finitamente generados, muchas estructuras algebraicas abstractas terminan comportándose de una forma muy similar a los números enteros, de modo que el pequeño teorema es susceptible de aplicarse con cierta generalidad en teoría de grupos.

La razón por la que el pequeño teorema es útil en diversos contextos es que proporciona información acerca de los números primos, siendo estos últimos los que intervienen en los campos citados en el párrafo anterior. Más concretamente, proporciona una condición necesaria para que un número entero sea primo, y por ende, puede utilizarse para garantizar que muchos enteros son compuestos. Desgraciadamente, el pequeño teorema no puede utilizarse para ratificar que un número es primo: existen enteros compuestos que cumplen la condición que este resultado impone. Este hecho ha motivado la introducción de nociones como pseudoprimo de Fermat o base pseudoprima (que hoy en día son básicas para entender la mayoría de tests de primalidad modernos como Rabin-Miller, Solovay-Strassen o AKS), y por supuesto, justifica el estudio de los números de Carmichael.

En este capítulo se presenta el pequeño teorema de Fermat y se definen las nociones del anterior párrafo (salvo la de número de Carmichael, que se reserva para el comienzo del Capítulo 3). Adicionalmente, se recoge una cadena de resultados relacionados con los conceptos anteriores, que culmina en el cálculo explícito del cardinal de bases pseudoprimas para un número entero compuesto (teorema de Baillie-Wagstaff). Argumentaremos por qué éste conduce de manera directa a la noción de número de Carmichael, que se desarrollará con detalle en el siguiente capítulo.

2.1. El pequeño teorema de Fermat

El pequeño teorema de Fermat puede enunciarse de la manera siguiente.

Teorema 2.1.1 (Fermat, 1640)**.** *Sea p un número primo y a un entero cualquiera. Entonces, $a^p - a$ es siempre divisible entre p.*

En aritmética modular, el enunciado anterior es equivalente a

$$a^p \equiv a \pmod{p}$$

Demostración. Sea p un número primo cualquiera. Demostramos que el resultado es cierto para todo entero positivo a, procediendo por inducción. Si $a = 1$, es claro que $1^p = 1 \equiv 1 \pmod{p}$.

Supongamos ahora que $a^p \equiv a \pmod{p}$ para un cierto entero positivo a, y veamos que $(1+a)^p \equiv 1 + a \pmod{p}$. Por el teorema del binomio,

$$(1+a)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \binom{p}{1} a + \cdots + \binom{p}{p-1} a^{p-1} + a^p \ ,$$

donde se ha utilizado que $\binom{p}{0} = \binom{p}{p} = 1$. Como $p | \binom{p}{k}$ para todo $1 \leq k \leq p-1$, porque $p \mid p!$ y $p \not| \, k!$, $p \not| \, (p-k)!$ por ser p primo, los términos intermedios se anulan $\pmod{p}$. Se sigue que

$$(1+a)^p \equiv 1 + a^p \pmod{p}$$

Haciendo uso de la hipótesis inductiva $a^p \equiv a \pmod{p}$, podemos reemplazar

$$(1+a)^p \equiv 1 + a^p \equiv 1 + a \pmod{p} \ ,$$

que demuestra el resultado para todo entero positivo. Por otra parte, como todo entero es congruente a un entero positivo $\pmod{p}$, el resultado se cumple para todo entero. □

Observación 2.1.2. Como el anillo $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un dominio de integridad para cualquier p primo, puede aplicarse la ley de cancelación para afirmar, en virtud del pequeño teorema de Fermat, que si $a \in (\mathbb{Z}/p\mathbb{Z})^*$ entonces $a^{p-1} \equiv 1 \pmod{p}$. Por esta razón es habitual encontrar el teorema anterior enunciado de la siguiente manera.

Dados un primo p y un entero a tales que $(p, a) = 1$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Corolario 2.1.3. *El anillo $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo.*

Demostración. Por la observación anterior,

$$a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p} \ ,$$

resultando que el inverso de a en $\mathbb{Z}/p\mathbb{Z}$ es precisamente a^{p-2}. Como el único a tal que $(p, a) \neq 1$ es precisamente el elemento neutro de la suma, $a = 0$, se tiene que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. □

Una aplicación inmediata del pequeño teorema es su posible uso como test de primalidad. Dado un entero positivo n, si existe alguún otro entero $0 < a < n$ tal que

$$a^{p-1} \not\equiv 1 \pmod{n} \ ,$$

el pequeño teorema garantiza que n no es primo. Pese a ello, el teorema no garantiza que los enteros cumpliendo la anterior congruencia sean primos.

A continuación se presenta un resultado que generaliza la idea del pequeño teorema a cualquier entero (no necesariamente primo). Fue obtenido por Eüler [Eü41], quien lo recogió en el siguiente teorema

Teorema 2.1.4 (Eüler)**.** *Sean a, n enteros positivos, con $(a, n) = 1$. Entonces*

$$a^{\varphi(n)} \equiv 1 \pmod{n} ,$$

donde $\varphi(n)$ es la función de Eüler.

Demostración. El conjunto de las clases residuales (mód n) de enteros primos con n constituye el bien conocido grupo de las unidades de $\mathbb{Z}/n\mathbb{Z}$, denotado por $(\mathbb{Z}/n\mathbb{Z})^*$. Por el teorema de Lagrange, el orden de cualquier $a \in (\mathbb{Z}/n\mathbb{Z})^*$ debe ser divisor de $\varphi(n)$. En consecuencia, si o es el orden del elemento a, existe un entero u tal que $ou = \varphi(n)$ y se tiene

$$a^{\varphi(n)} = a^{ou} = (a^o)^u \equiv 1^u = 1 \pmod{n} ,$$

lo que concluye la demostración. □

Observación 2.1.5. Cabe destacar que una demostración equivalente a la realizada para el Teorema 2.1.4 podría haberse realizado para el Teorema 2.1.1. La razón de haber optado por una diferente es ceñirse al contexto histórico en que el pequeño teorema fue demostrado.

2.2. Pseudoprimos de Fermat

2.2.1. Definición de pseudoprimo de Fermat

El pequeño teorema de Fermat proporciona una condición necesaria para que un entero sea primo. Sin embargo, existen enteros que, sin ser primos, satisfacen la congruencia que éste impone para algunas bases. Los siguientes ejemplos muestran algunos de estos números.

Ejemplo 2.2.1 (Enteros impares y compuestos)**.** *Sea n un entero impar y compuesto. Dado que $n - 1 \equiv -1 \pmod{n}$, se sigue*

$$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv ((-1)^2)^{(n-1)/2} \equiv 1^{(n-1)/2} \equiv 1 \pmod{n} .$$

Por lo que la condición del pequeño teorema es satisfecha para el par n y $a = n - 1$, sea n primo o no.

Ejemplo 2.2.2. *Sea $n = 341 = 11{\cdot}31$. No es difícil comprobar que $2^{10} = 1024 = 1023{+}1 = 341 \cdot 3 + 1 \equiv 1 \pmod{341}$. En consecuencia,*

$$2^{341-1} = 2^{34\cdot 10} \equiv \left(2^{10}\right)^{34} \equiv 1^{34} \equiv 1 \pmod{341}.$$

Por ello, pese a que n es compuesto, el par $n = 341$, $a = 2$ satisface la condición del pequeño teorema.

Los ejemplos precedentes motivan la introducción de la noción de *pseudoprimo de Fermat*.

Definición 2.2.3. Sean n y a dos enteros tales que $1 \leq a \leq n-1$ y $(n, a) = 1$. Diremos que n es un *pseudoprimo de Fermat para la base* a si es compuesto y la congruencia

$$a^{n-1} \equiv 1 \pmod{n}$$

se satisface. En estas condiciones, diremos que a es un mentiroso de Fermat para n. En caso de que la congruencia anterior no se cumpla, diremos que a es un testigo de Fermat.

Definición 2.2.4. Los pseudoprimos para la base 2 se conocen como números de Poulet.

De ahora en adelante, emplearemos meramente el término pseudoprimo para referirnos a un pseudoprimo de Fermat (pese a que existen diferentes familias de pseudoprimos, no hablaremos de ninguna otra), y de igual modo escribiremos solamente base testigo o mentirosa.

2.2.2. Construcción de pseudoprimos para una base

Resulta natural preguntarse por la cantidad de pseudoprimos que existe para una base dada, en caso de existir alguno. De igual modo, sería conveniente conocer el número exacto de bases para las que un entero positivo dado es pseudoprimo. Los resultados siguientes responden a la primera de las preguntas. No solo garantizan la existencia de pseudoprimos para cualquier base sino que además confirman la existencia de infinitos de ellos.

Comencemos con el caso sencillo de los números de Poulet. Las siguientes dos definiciones resultarán útiles para demostrar la existencia de infinitos números de Poulet.

Definición 2.2.5 (Números de Fermat)**.** Sea n un entero no negativo. El n-ésimo [1] *número de Fermat*, denotado por F_n, se define como

$$F_n = 2^{2^n} + 1 \ .$$

Fermat conjeturó que todos estos números serían primos [Rib12], y se convenció de ello comprobando que efectivamente los primeros lo eran. Sin embargo, el crecimiento doblemente exponencial de los mismos le impidió manejar términos posteriores a F_4. En 1732, Eüler calculó $F_5 = 4294967297$ y observó que $4294967297 = 641 \cdot 6700417$, en contra de la creencia de Fermat. Sin embargo, el conocimiento que a día de hoy se tiene de los números de Fermat sigue siendo muy limitado. Se conoce solamente la factorización de los 12 primeros, y es un problema abierto decidir si existen infinitos números de Fermat que son primos o si, en contra, sólo existen los mismos 5 que ya Fermat conocía, F_0, F_1, F_2, F_3 y F_4.

Definición 2.2.6 (Números de Mersenne)**.** Sea n un entero no negativo. El n-ésimo número de Mersenne, denotado por M_n, se define como

$$M_n = 2^n - 1 \ .$$

De forma similar a Fermat, el filósofo francés Marin Mersenne [Rib12] conjeturó en el siglo XVII que todos los números de Mersenne, satisfaciendo la condición de que n es primo, debían ser también primos. Al igual que con Fermat la conjetura resultó ser falsa, pues $M_{11} = 2047 = 23 \cdot 89$. Los números de Mersenne siguen siendo fruto de investigación

[1] Conviene notar que, con esta notación, F_1 no es el primer número de Fermat ya que existe el "0−ésimo", $F_0 = 2 + 1 = 3$.

hoy en día, y múltiples preguntas acerca de su naturaleza siguen abiertas. En concreto, no se dispone de ninguna prueba de la existencia de infinitos números de Mersenne primos.

Pese a las preguntas abiertas en relación a estas dos familias de números, existen muchos resultados útiles que los involucran. El teorema siguiente [KLS13] garantiza que, en algunos casos, F_m y M_p son números de Poulet.

Teorema 2.2.7. *Sea F_m y M_p dos números de Fermat y Mersenne respectivamente, donde p es primo. Si alguno de ellos es compuesto, entonces es un número de Poulet.*

Demostración. Comencemos viendo que la afirmación sobre los números de Fermat es cierta. Notemos que

$$2^{F_m-1} = 2^{2^m} \equiv -1 \pmod{F_m} .$$

Denotando $k = 2^m - m > 0$, resulta claro

$$2^{2^{2^m}} = 2^{2^m \cdot 2^k} = (2^{2^m})^{2^k} \equiv (-1)^{2^k} = 1 \pmod{F_m} .$$

Entonces, si F_m es compuesto es también pseudoprimo para la base 2. Pasemos al caso de los números de Mersenne. De nuevo, es sencillo comprobar que $(M_p - 1)/2 = 2^{p-1} - 1$. Además, por el pequeño teorema de Fermat se tiene

$$2^{p-1} - 1 \equiv 0 \pmod{p} ,$$

así que existe un natural s tal que $(M_p - 1)/2 = p \cdot s$. Por lo tanto,

$$2^{(M_p-1)/2} = 2^{p \cdot s} = (2^p)^s \equiv 1^s = 1 \pmod{M_p} ,$$

donde se ha utilizado que $2^p \equiv 1 \pmod{M_p}$. Finalmente,

$$2^{M_p-1} = (2^{(M_p-1)/2})^2 \equiv 1^2 = 1 \pmod{M_p} ,$$

y si M_p es compuesto es también un número de Poulet. □

Si bien el Teorema anterior es útil para generar algunos números de Poulet de manera sencilla, el desconocimiento acerca de cúantos números de Fermat o Mersenne compuestos hay, así como las dificultades encontradas en la comprobación de si son primos, no permite garantizar la existencia de infinitos números de Poulet. Los siguientes resultados [Rib12] conducen a un algoritmo que sí permite probar de una forma constructiva la existencia de infinitos números de Poulet.

Lema 2.2.8. *Sea n un entero positivo. Entonces $F_n - 2 = F_{n-1} \cdot F_{n-2} \cdot \cdots \cdot F_1 \cdot F_0$.*

Demostración. Sea F_n el n-ésimo número de Fermat. Procedemos por inducción. En efecto, para $n = 1$

$$F_1 - 2 = 2^{2^1} - 1 = 3$$
$$F_0 = 2^{2^0} + 1 = 3 ,$$

y la afirmación se cumple. Suponiendo ahora el resultado cierto para un entero positivo n, probamos que lo sigue siendo para $n + 1$. No es difícil comprobar

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = 2^{2^n \cdot 2} - 1 = (2^{2^n} - 1) \cdot (2^{2^n} + 1) = (F_n - 2) \cdot F_n$$

Por la hipótesis de inducción se tiene que $F_n - 2 = F_{n-1} \cdot \ldots \cdot F_1 \cdot F_0$, lo que prueba la igualdad para todo entero positivo n. □

Lema 2.2.9. *Sean n, m dos enteros no negativos distintos. Entonces $(F_n, F_m) = 1$.*

Demostración. Podemos asumir que $n < m$. Por el Lema 2.2.8, se cumple que $F_n|(F_m - 2)$. En consecuencia, cualquier primo p dividiendo a F_n ha de dividir también a $F_m - 2$. Como todos los números de Fermat son impares también debe serlo p, de modo que $p \not| F_m$. □

Observación 2.2.10. A modo de curiosidad, el Lema 2.2.9 en conjunto con el Teorema Fundamental de la Aritmética proporciona una prueba alternativa a la existencia de infinitos números primos.

El siguiente resultado [Cip04] conduce a al algoritmo mencionado en la página anterior. Éste permite generar infinitos números de Poulet, coprimos dos a dos.

Teorema 2.2.11. *Si $n_r > n_{r-1} > \ldots > n_1 > 1$ son enteros, el número $N = F_{n_r} \cdot F_{n_{r-1}} \cdot \ldots \cdot F_{n_1}$ es un número de Poulet si, y sólo si, $2^{n_1} > n_r$.*

Demostración. Dado un entero positivo m, del Lema 2.2.8 se sigue que

$$2^{2^{m+1}} \equiv 1 \pmod{F_m} ,$$

siendo además $m + 1$ la menor potencia para la que se da la congruencia. Esto implica que el orden de 2 (mód F_m) es exactamente 2^{m+1}. En consecuencia, como los números de Fermat son coprimos dos a dos, basta con aplicar el teorema chino de los restos para comprobar que el orden de 2 (mód N) es el mínimo común múltiplo del orden de 2 módulo los números de Fermat de la descomposición. De nuevo éste vale 2^{n_r+1}, y por tanto

$$2^{N-1} \equiv 1 \pmod{N} \quad \text{si, y solo si} \quad 2^{n_r+1} \mid N - 1 .$$

Por otra parte,

$$N = (2^{2^{n_r}} + 1) \cdot (2^{2^{n_{r-1}}} + 1) \cdot \cdots \cdot (2^{2^{n_1}} + 1) = 2^{2^{n_1}} \cdot Q + 1 ,$$

donde la última igualdad puede escribirse porque el único término de la expansión que no es divisible entre $2^{2^{n_1}}$ es el correspondiente al producto de exactamente r unos. Más aún, Q es impar por ser la suma de potencias de 2 y un único 1. Inmediatamente de la igualdad anterior se deduce

$$N - 1 = 2^{2^{n_1}} \cdot Q$$

Finalmente, el hecho de que $2^{n_r+1} \mid N - 1$ es equivalente a que $2^{n_1} > n_r$, lo que concluye la demostración. □

El Teorema 2.2.11 permite construir un conjunto infinito de números de Poulet, escogiendo listas finitas de números naturales satisfaciendo la condición $2^{n_1} > n_r$ y calculando N. Si además estas listas se toman disjuntas dos a dos, el Lema 2.2.9 garantiza que los pseudoprimos generados serán coprimos dos a dos.

Hasta ahora se han dado métodos que permiten la construcción de pseudoprimos de Poulet (i.e. para la base 2). El resultado que se presenta a continuación, también debido a Cipolla, da respuesta a la pregunta sobre la existencia de pseudoprimos para cualquier otra base $a > 2$. Más aún, éste permite construir una familia infinita de pseudoprimos para la base escogida.

Teorema 2.2.12. *Sea $a \geq 2$ un entero y p un primo impar tal que $p \nmid a(a^2-1)$. Sean*

$$n_1 = \frac{a^p - 1}{a-1} \quad , \quad n_2 = \frac{a^p + 1}{a+1} \ .$$

Entonces, $n = n_1 \cdot n_2$ es un pseudoprimo para la base a.

Demostración. Para ver que n es compuesto, basta con demostrar que $n_1, n_2 > 1$. Esto es claro teniendo en cuenta que

$$n_1 = \frac{a^p - 1}{a-1} = a^{p-1} + a^{p-2} + \ldots + a + 1 > 1$$

$$n_2 = \frac{a^p + 1}{a+1} = a^{p-1} - a^{p-2} + \ldots - a + 1 = 1 + \sum_{i=1}^{(p-1)/2} (a^{2i} - a^{2i-1}) >$$

$$> 1 + \sum_{i=1}^{(p-1)/2} (a^{2i-1} - a^{2i-1}) = 1 \ .$$

Además, tanto n_1 como n_2 son iguales a la suma de un número par de términos de la misma paridad y una unidad, de modo que n es impar. Se sigue que

$$n_1 \cdot (a-1) = a^p - 1 \equiv (a-1)^p \equiv a - 1 \pmod{p}$$
$$n_2 \cdot (a+1) = a^p + 1 \equiv (a+1)^p \equiv a + 1 \pmod{p} \ ,$$

donde las últimas congruencias se satisfacen por ser p primo. Como además se cumple que $p \nmid (a^2-1) = (a+1)(a-1)$, se verifica

$$n_1 \equiv 1 \pmod{p} \quad , \quad n_2 \equiv 1 \pmod{p}$$

En consecuencia, $n = n_1 \cdot n_2 \equiv 1 \pmod{p}$ y, por tanto, $n - 1 = 2pk$.

Por otra parte, es claro que si $a^{2p} \equiv 1 \pmod{n}$ entonces n debe ser pseudoprimo para la base a, pues en tal caso

$$a^{n-1} = a^{2pk} = \left(a^{2p}\right)^k \equiv 1^k \equiv 1 \pmod{n} \ .$$

Sin embargo, se verifica

$$n = n_1 \cdot n_2 = \frac{a^{2p} - 1}{a^2 - 1} \equiv 0 \pmod{n} \ ,$$

de modo que ha de cumplirse que $a^{2p} - 1 \equiv 0 \pmod{n}$ y la demostración queda completa. □

En virtud del teorema anterior, dados una base a y un primo p que no se encuentre en la factorización de $a(a^2-1)$, es posible generar un pseudoprimo para a. Como el conjunto de números primos en las condiciones anteriores es infinito, también lo es el número de pseudoprimos para la base a.

2.2.3. Cálculo del cardinal de bases mentirosas para un pseudoprimo

Abordamos ahora la cuestión acerca del cálculo de bases mentirosas para un determinado entero compuesto n. Comenzamos definiendo el conjunto

$$\mathrm{B}_{psp}(n) := \{1 \leq a \leq n : \ a^{n-1} \equiv 1 \pmod{n}\} \ , \tag{2.1}$$

formado por todas las bases mentirosas de n. Obviamente, para cualquier n compuesto se cumple que $1 \in \mathrm{B}_{psp}(n)$, y como hemos visto en el Ejemplo 2.2.1, si además n es impar se tiene $n-1 \in \mathrm{B}_{psp}(n)$. Por tanto, sabemos que $\mathrm{B}_{psp}(n)$ es no vacío. El objetivo de esta sección es demostrar el teorema de Baillie-Wagstaff, que proporciona una forma para calcular de fórmula explícita $|\mathrm{B}_{psp}(n)|$ a partir de la factorización de n.

A fin de simplificar la notación en los resultados siguientes, en lo sucesivo denotaremos por f_n al polinomio

$$f_n(X) = X^n - 1 \ ,$$

donde n es un entero positivo. Del mismo modo, llamaremos simplemente "congruencia" a cualquier "ecuación polinomial en congruencias", esto es, a cualquier ecuación de la forma

$$g(X) \equiv 0 \pmod{m} \ ,$$

donde g es un polinomio y m un entero. Además, todos los polinomios se consideran elementos de $\mathbb{Z}[X]$.

Definición 2.2.13. Sea $g(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ un polinomio y m un entero. Sea $0 \leq j \leq n$ el mayor entero tal que $a_j \not\equiv 0 \pmod{m}$. Diremos que el grado de la congruencia (mód m) es j. Si no existe j en esas condiciones, no se asigna grado a la congruencia.

Proposición 2.2.14. [NZM13] Sea p un primo. La congruencia $g(X) \equiv 0 \pmod{p}$ de grado $n \pmod{p}$ tiene a lo sumo n soluciones.

Demostración. Se procede por inducción.

Si $n = 0$, se tiene $g(X) = a_0 \equiv 0 \pmod{p}$, sin solución.

Si $n = 1$, se tiene $g(X) = a_1 X + a_0 \equiv 0 \pmod{p}$. Como $\mathbb{F}_p$ es cuerpo, tiene una única solución.

Supuesto el resultado correcto para toda congruencia de grado menor a n, se prueba para grado n. Sea $g(X) \equiv 0 \pmod{p}$ una congruencia de grado n. Supongamos que tiene más de n soluciones y consideremos $u_1, u_2, \ldots, u_{n+1}$ una familia de cardinal $n+1$ de las mismas. Se define el polinomio

$$h(X) = g(X) - a_n(X - u_1)(X - u_2)\ldots(X - u_n) \ ,$$

donde a_n es el coeficiente director de g. Si alguno de los coeficientes de h no es divisible por p, entonces la congruencia tiene asignada un grado. En este caso, tal grado debe ser menor que n. Sin embargo, la congruencia tiene al menos las soluciones $u_1, u_2, \ldots, u_n$ por construcción, en contra de la hipótesis inductiva.

Por lo tanto, debe ser $h(X) \equiv 0 \pmod{p}$, resultando que todo entero es solución. En particular, u_{n+1} lo es. Sin embargo, se tiene que

$$h(u_{n+1}) = a_n(u_{n+1} - u_1)(u_{n+1} - u_2)\ldots(u_{n+1} - u_n) \not\equiv 0 \pmod{p} \ ,$$

llegándose otra vez a una contradicción. Por todo ello, no es posible que una congruencia de grado n tenga más de n soluciones, lo que concluye la demostración. □

Lema 2.2.15. *Sean a, b y n enteros, con $a, b > 0$. Denotemos $d = (a, b)$. Si ξ es una solución común a las congruencias $f_a(X) \equiv 0 \pmod{n}$ y $f_b(X) \equiv 0 \pmod{n}$, entonces también es solución de $f_d(X) \equiv 0 \pmod{n}$.*

Demostración. Por ser ξ solución de las congruencias $f_a(X) \equiv 0 \pmod{n}$ y $f_b(X) \equiv 0 \pmod{n}$, se cumple que

$$\xi^a \equiv 1 \pmod{n} \ , \ \xi^b \equiv 1 \pmod{n} \ .$$

Por otra parte, el teorema de Bézout garantiza la existencia de enteros α, β tales que la igualdad

$$\alpha a + \beta b = d \ ,$$

se satisface. Se sigue que

$$\xi^d = \xi^{\alpha a + \beta b} = \xi^{\alpha a} \cdot \xi^{\beta b} \equiv (\xi^a)^\alpha \cdot (\xi^b)^\beta \equiv 1 \pmod{n} \ ,$$

lo que implica que ξ es también solución de $f_d(X) \equiv 0 \pmod{n}$. □

Proposición 2.2.16. [NZM13] Sea k un entero positivo y p un primo. El conjunto de soluciones de la ecuación $f_k(X) \equiv 0 \pmod{p}$ tiene cardinal $(k, p-1)$.

Demostración. Comencemos viendo que si $u|(p-1)$ entonces $f_u(x) \equiv 0 \pmod{p}$ tiene u exactamente u soluciones. Tomando e tal que $p - 1 = eu$, se tiene

$$f_{p-1}(X) = f_u(X) \cdot (1 + X^u + \ldots + X^{u(e-1)}) \ .$$

Por el pequeño teorema de Fermat la ecuación $f_{p-1}(X) \equiv 0 \pmod{p}$ tiene $p-1$ soluciones, cada una de las cuales debe ser solución de alguna de las congruencias

$$f_u(X) \equiv 0 \pmod{p} \quad \text{o} \quad 1 + X^h + \ldots + X^{u(e-1)} \equiv 0 \pmod{p} \ ,$$

ya que $\mathbb{Z}/p\mathbb{Z}$ es un dominio de integridad. Como la Proposición 2.2.14 garantiza que el conjunto de soluciones de una congruencia está acotado superiormente por su grado, y en conjunto las soluciones de ambas deben sumar al menos $p - 1$, la única posibilidad es que tengan exactamente u y $u(e-1)$ soluciones sin ninguna común. En particular, llamando $d = (k, p-1)$, la congruencia $f_d(X) \equiv 0 \pmod{p}$ tiene exactamente d soluciones.

Sea ξ una solución de la congruencia $f_k(X) \equiv 0 \pmod{p}$. Es claro que ésta es también solución de $f_{p-1}(X) \equiv 0 \pmod{p}$. Entonces, por el Lema 2.2.15 todas ellas son soluciones de $f_d(X) \equiv 0 \pmod{p}$. Razonando con el mismo argumento del comienzo de la demostración se tiene que $f_d(X) \mid f_k(X)$, de modo que todas las soluciones de $f_d(X) \equiv 0 \pmod{p}$ lo son también de $f_k(X) \equiv 0 \pmod{p}$. En consecuencia, el conjunto de soluciones de ambas congruencias es el mismo, de cardinal d. □

Observación 2.2.17. Sean k, s dos enteros tales que $0 \leq k < p-1$ y $s \equiv k \pmod{p-1}$. Entonces, por el pequeño teorema de Fermat

$$f_s(X) = X^s - 1 = X^{q\cdot(p-1)+k} - 1 = (X^{p-1})^q X^k - 1 \equiv X^k - 1 = f_k(X) \pmod{p} \ ,$$

de modo que las soluciones de la congruencia son las mismas sea el exponente k o s. Por lo tanto, la Proposición 2.2.16 puede enunciarse escogiendo un k tal que $1 \leq k \leq p-1$.

Corolario 2.2.18. *Dado un primo p, $\mathbb{F}_p{}^*$ es cíclico.*

Demostración. Escogiendo $n = p - 1$, la Proposición 2.2.16 garantiza que la congruencia $f_{p-1} \equiv 0 \pmod{p}$ tiene $p - 1$ soluciones. Por lo tanto, el orden de todas las soluciones de la congruencia debe ser menor que $p - 1$. Veamos que debe existir alguna primitiva.

Si todas ellas tuvieran orden menor a $p - 1$, existiría $u < p - 1$ de modo que la congruencia $f_u \equiv 0 \pmod{p}$ tiene al menos $p - 1$ soluciones. Sin embargo, esto no es posible por la Proposición 2.2.16. Por lo tanto alguna de ellas debe tener orden $p-1$ y $\mathbb{F}_p$ es cíclico. □

Corolario 2.2.19. *[HW79] Sea p un primo y k, α dos enteros positivos, con $\alpha > 1$. Supongamos que además $(p, k) = 1$. Entonces, existe una biyección entre los conjuntos de soluciones de las congruencias $f_k(X) \equiv 0 \pmod{p^\alpha}$ y $f_k(X) \equiv 0 \pmod{p^\beta}$, para todo $1 \leq \beta \leq \alpha$.*

Demostración. Sea ξ una solución de la congruencia $f_k(X) \equiv 0 \pmod{p^\alpha}$. También es solución de $f_k(X) \equiv 0 \pmod{p^{\alpha-1}}$. Además, es de la forma

$$\xi = \eta + sp^{\alpha-1} \quad , \quad 0 \leq s < p \ ,$$

donde η es una solución de $f_k(X) \equiv 0 \pmod{p^{\alpha-1}}$ tal que $0 \leq \eta < p^{\alpha-1}$.

Expandiendo como serie de Taylor, se encuentra que

$$\begin{aligned} f(\xi) = f(\eta + sp^{\alpha-1}) = f(\eta) + sp^{\alpha-1}f'(\eta) + \frac{1}{2}s^2p^{2\alpha-2}f''(\eta) + \ldots \equiv \\ \equiv f(\eta) + sp^{\alpha-1}f'(\eta) \pmod{p^\alpha} \ , \end{aligned}$$

ya que para todo $m > 1$ se tiene que $m\alpha - m = m(\alpha - 1) > \alpha$, y los coeficientes

$$\frac{f^{(m)}(\eta)}{m!}$$

son enteros. Además, por ser ξ una solución de $f_k(X) \equiv 0 \pmod{p^\alpha}$,

$$f(\xi) = 0 \equiv f(\eta) + sp^{\alpha-1}f'(\eta) \pmod{p^\alpha} \iff sf'(\eta) \equiv -\frac{f(\eta)}{p^{\alpha-1}} \pmod{p^\alpha} \ . \tag{2.2}$$

Por otra parte, $f'(X) = kX^{k-1}$. Como $(p, k) = 1$, se tiene que $kX^{k-1} \not\equiv 0 \pmod{p^{\alpha-1}}$, y en consecuencia $sf'(\eta) \not\equiv 0 \pmod{p}$.

Por lo tanto existe un único $s \pmod{p}$ que satisface la congruencia (2.2), de modo que para cada solución de $f_k \equiv 0 \pmod{p^\alpha}$ existe una única solución de $f_k \equiv 0 \pmod{p^{\alpha-1}}$ y existe una biyección entre ambos conjuntos de soluciones.

Los mismos argumentos son válidos para concluir, de forma iterativa, que el cardinal de los conjuntos de soluciones de las congruencias $f_k(X) \equiv 0 \pmod{p^\alpha}$ y $f_k(X) \equiv 0 \pmod{p^\beta}$ es el mismo para $1 \leq \beta \leq \alpha$, lo que completa la demostración. □

Enunciamos a continuación el teorema de Baillie-Wagstaff, que proporciona una forma explícita de calcular el cardinal de $B_{psp}(n)$.

Teorema 2.2.20. *[BW80] Sea $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ un entero compuesto. Entonces,*

$$|B_{psp}(n)| = \prod_{i=1}^{k} (n - 1, p_i - 1)$$

Demostración. Por la Proposición 2.2.16, el conjunto de soluciones de la congruencia

$$f_{n-1}(X) \equiv 0 \pmod{p_i}$$

tiene cardinal $(n-1, p_i - 1)$. Además, para cada $1 \leq i \leq k$, como $p_i | n$ se tiene que $(p_i, n-1) = 1$, de modo que el Corolario 2.2.19 garantiza que el conjunto de soluciones de

$$f_{n-1}(X) \equiv 0 \pmod{p_i^{\alpha_i}}$$

tiene cardinal $(n-1, p_i - 1)$. Basta con aplicar ahora el teorema chino de los restos para concluir que el cardinal de $B_{psp}(n)$ es

$$|B_{psp}(n)| = \prod_{i=1}^{k} (n-1, p_i - 1) \ .$$

□

Dado un entero compuesto n cuya factorización en primos es conocida, el Teorema 2.2.20 hace posible calcular el número de bases para las que n es pseudoprimo, tal y como muestra el siguiente ejemplo.

Ejemplo 2.2.21 (Bases mentirosas para algunos compuestos)**.**

i) $n_1 = 36 = 2^2 \cdot 3^2$
$|B_{psp}(36)| = (36-1, 2-1)(36-1, 3-1) = 1$,

de modo que $n_1 = 36$ *es pseudoprimo para una única base,* $a = 1$*.*

ii) $n_2 = 616 = 2^3 \cdot 7 \cdot 11$
$|B_{psp}(616)| = (616-1, 2-1)(616-1, 7-1)(616-1, 11-1) = 3 \cdot 5 = 15$,

de modo que $n_2 = 616$ *es pseudoprimo para* 15 *bases. Además, resulta que*

$$B_{psp}(616) = \{1, 9, 25, 81, 113, 137, 169, 177, 225, 289, 345, 361, 401, 449, 529\}$$

iii) $n_3 = 77 = 7 \cdot 11$
$|B_{psp}(77)| = (77-1, 7-1)(77-1, 11-1) = 2 \cdot 2 = 4$,

de modo que $n_3 = 77$ *es pseudoprimo para* 4 *bases. Además, resulta que*

$$B_{psp}(77) = \{1,\ 34,\ 43,\ 76\}$$

iv) $n_4 = 561 = 3 \cdot 11 \cdot 17$
$|B_{psp}(561)| = (561-1, 3-1)(561-1, 11-1)(561-1, 17-1) = 2 \cdot 10 \cdot 16 = 320$,

de modo que $n_4 = 561$ *es pseudoprimo para* 320 *bases. Por otra parte, se encuentra fácilmente que* $\varphi(561) = 2 \cdot 10 \cdot 16 = 320$*. Sumado con lo anterior, esto significa que* 561 *es pseudoprimo para todos los elementos de* $(\mathbb{Z}/561\mathbb{Z})^*$*.*

El último caso del Ejemplo 2.2.21 ($n_4 = 561$) muestra un ejemplo de un número que es pseudoprimo para todas sus bases. Esta condición es justamente la que define a los números de Carmichael, que se estudian en este trabajo. En los capítulos posteriores se analizan en mayor profundidad propiedades elementales de este tipo de números, así como algún resultado más avanzado que los involucra.

Capítulo 3

Números de Carmichael

Tal y como muestra el último caso del Ejemplo 2.2.21 del capítulo anterior, existen enteros n tales que $|B_{psp}(n)| = \varphi(n)$. En otras palabras, hay números que resultan ser pseudoprimos para todas sus posibles bases. Los números de este tipo fueron primeramente estudiados por Alwin Korselt [Kor99], quien logró caracterizarlos con una condición necesaria y suficiente pese a que se vio incapaz de encontrar algún ejemplo de los mismos. Pocos años después, Robert Daniel Carmichael los estudió de forma independiente. Publicó un artículo [Car12] en *The American Mathematical Monthly*, en febrero de 1912, donde demostró que el recíproco del pequeño teorema de Fermat no es cierto aportando varios enteros que eran pseudoprimos para todas las bases. Entre sus ejemplos, se encuentran el 561, 2821, 8911 y 15841. Por haber logrado encontrar ejemplos de los mismos, y haber estudiado algunas de sus propiedades, hoy en día estos números llevan su nombre.

En este capítulo nos centramos en el estudio de los números de Carmichael. En las dos primeras secciones deducimos dos caracterizaciones de esta familia de números siguiendo caminos diferentes: el criterio de Korselt y la función de Carmichael. Si observamos la Tabla 3.1, que recoge los 20 primeros números de Carmichael con sus factorizaciones, a simple vista podemos distinguir algunas peculiaridades en su forma. Por ejemplo todos los números listados son impares, y todos ellos tienen al menos 3 factores primos distintos. En la última sección de este capítulo abordaremos estas dos cuestiones, junto con otras similares.

n	n-ésimo número de Carmichael	n	n-ésimo número de Carmichael
1	$561 = 3 \cdot 11 \cdot 17$	11	$41041 = 7 \cdot 11 \cdot 13 \cdot 41$
2	$1105 = 5 \cdot 13 \cdot 17$	12	$46657 = 13 \cdot 37 \cdot 97$
3	$1729 = 7 \cdot 13 \cdot 19$	13	$52633 = 7 \cdot 73 \cdot 103$
4	$2465 = 5 \cdot 17 \cdot 29$	14	$62745 = 3 \cdot 5 \cdot 47 \cdot 89$
5	$2821 = 7 \cdot 13 \cdot 31$	15	$63973 = 7 \cdot 7 \cdot 19 \cdot 37$
6	$6601 = 7 \cdot 23 \cdot 31$	16	$75361 = 11 \cdot 13 \cdot 17 \cdot 31$
7	$8911 = 7 \cdot 19 \cdot 67$	17	$101101 = 7 \cdot 11 \cdot 13 \cdot 101$
8	$10585 = 5 \cdot 29 \cdot 73$	18	$115921 = 13 \cdot 37 \cdot 241$
9	$15841 = 7 \cdot 31 \cdot 73$	19	$126217 = 7 \cdot 13 \cdot 19 \cdot 73$
10	$29341 = 13 \cdot 37 \cdot 61$	20	$162401 = 17 \cdot 41 \cdot 233$

Tabla 3.1: Los 20 primeros números de Carmichael y sus factorizaciones.

3.1. Números de Carmichael y el criterio de Korselt

Como ya se ha explicado, la propiedad que distingue a estos números es la que se recoge en la siguiente definición.

Definición 3.1.1 (Número de Carmichael)**.** Sea n un entero positivo y compuesto. Se dice que n es un número de Carmichael si es pseudoprimo para todas las bases.

De forma equivalente, n es un número de Carmichael si $|B_{psp}(n)| = \varphi(n)$.

El primer resultado obtenido en relación a estos números fue la caracterización que Korselt encontró. Ésta se recoge en el siguiente teorema.

Teorema 3.1.2 (Korselt, 1899)**.** *Sea n un entero compuesto. Las dos condiciones siguientes son equivalentes:*

1. *El entero n es un número de Carmichael*
2. *El entero n es libre de cuadrados y, para cualquier divisor primo p de n, se cumple que $p-1|n-1$.*

A este resultado se le conoce como el criterio de Korselt.

Demostración. Sea n un número de Carmichael y p uno de sus divisores primos. Comencemos viendo que es libre de cuadrados. Es claro que existe una descomposición de n tal que $n = p^k \cdot n'$, donde $k \geq 1$ y $(p, n') = 1$. Demostramos que $k = 1$ por reducción al absurdo.

Supongamos que $k > 1$, caso en el que $p^2|n$. Por el teorema chino de los restos, existe un único $a \in \mathbb{Z}/n\mathbb{Z}$ tal que

$$a \equiv 1 + p \pmod{p^k} \quad , \quad a \equiv 1 \pmod{n'} \ .$$

En ese caso $(a, n) = 1$, de modo que por ser n un número de Carmichael se tiene

$$a^{n-1} \equiv 1 \pmod{n} \ .$$

En consecuencia, se cumple también que

$$(1+p)^{n-1} \equiv 1 \pmod{p^2} \ .$$

El teorema del binomio garantiza

$$(1+p)^{n-1} \equiv 1 + (n-1)p \pmod{p^2} \ ,$$

pero como $n - 1 \equiv -1 \pmod{p^2}$, se verifica

$$(1+p)^{n-1} \equiv 1 - p \pmod{p^2} \ .$$

En consecuencia, se obtiene

$$1 \equiv 1 - p \pmod{p^2} \ ,$$

que es claramente un absurdo. Por ello, solo es posible que $k = 1$ y n sea libre de cuadrados.

Veamos que $p-1|n-1$. Como n es libre de cuadrados, $(n/p, p) = 1$. Sea b un elemento primitivo primitivo de $\mathbb{F}_p$ (existe por el Corolario 2.2.18). El teorema chino de los restos garantiza que existe un único $a \in \mathbb{Z}/p\mathbb{Z}$ tal que

$$a \equiv b \pmod{p} \ , \ a \equiv 1 \pmod{n/p} \ .$$

Por este mismo teorema es fácil ver que $a^{p-1} \equiv 1 \pmod{n}$, y por ser n un número de Carmichael debe tenerse que $p-1|n-1$.

Sea ahora $n > 2$ un entero compuesto y libre de cuadrados tal que $p-1|n-1$ para cada p primo divisor de n. Dado $a \in (\mathbb{Z}/n\mathbb{Z})^*$, el pequeño teorema de Fermat garantiza que $a^{p-1} \equiv 1 \pmod{p}$, para todo p divisor primo de n. Por lo tanto, se cumple que $a^{n-1} \equiv 1 \pmod{p}$. En consecuencia, $a^{n-1} \equiv 1 \pmod{n}$, resultando que n es un número de Carmichael. □

Como consecuencia del teorema anterior, si n es un número de Carmichael y $\{p_i : 1 \leq i \leq k\}$ es el conjunto de sus divisores primos, podremos escribir $n = \prod_{i=1}^{k} p_i$ por ser n libre de cuadrados.

El siguiente teorema confirma que el pequeño teorema de Fermat no es un test de primalidad válido, ya que todos los números de Carmichael lo pasan. Éste puede entenderse como una definición alternativa de los números de Carmichael. Sin embargo, resulta ser ligeramente más fuerte que la que hemos introducido aquí, y por tanto debemos demostrar su equivalencia.

Corolario 3.1.3. *Un entero compuesto n es un número de Carmichael si, y sólo si, se satisface la congruencia $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.*

Demostración. Sea n un entero compuesto. Es evidente que si n es tal que $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$, en el caso de que $(a, n) = 1$ puede cancelarse a ambos lados a (existe un inverso de a) para obtener $a^{n-1} \equiv 1 \pmod{n}$, resultando que n es un número de Carmichael.

Para el recíproco, si n es un número de Carmichael, el criterio de Korselt garantiza que es libre de cuadrados. En consecuencia, para ver que $a^n \equiv a \pmod{n}$ basta con probar que, para cada uno de sus divisores primos p, se tiene

$$a^n \equiv a \pmod{p}.$$

Esta condición se satisface de forma trivial si $a \equiv 0 \pmod{p}$. Por otra parte, si $(p, a) = 1$ el pequeño teorema de Fermat afirma que $a^{p-1} \equiv 1 \pmod{p}$. Teniendo en cuenta que por el criterio de Korselt se tiene $p-1|n-1$, se sigue que $a^{n-1} \equiv 1 \pmod{p}$. Finalmente, $a^n \equiv a \pmod{p}$. □

Aunque es cierto que los números de Carmichael son considerados primos por el pequeño teorema de Fermat como test de primalidad, la calidad del test está íntimamente relacionada de la "cantidad" de números de Carmichael que existan. Si la densidad de los números de Carmichael es baja (i.e. hay "pocos" números de Carmichael), dado un entero n que pasa el test sería razonable pensar que es un número primo. Volviendo a la Tabla 3.1, parece que en efecto éste es el caso: solo hay 10 de ellos por debajo de 40000, y 20 por debajo de 162402 (si el lector desea más información de este tipo acuda a la Tabla 5.1 en la página 46, que contiene la cantidad de números de Carmichael por debajo de 10^m, con $m = 3, 4, \ldots, 16$). Más aún, si resultara que solo existe una cantidad finita de números de Carmichael el test sería válido a partir del último número de la lista.

Por todo lo anterior, comprender el rango de validez del pequeño teorema como test de primalidad es una de las motivaciones para estudiar el crecimiento y la densidad de los números de Carmichael sobre los números reales. Las cuestiones planteadas en este párrafo se desarrollarán en el Capítulo 5.

3.2. La función de Carmichael

El estudio que Carmichael realizó en su primer artículo acerca de los números que llevan su nombre se encontraba apoyado por completo en una cierta función, hoy conocida como función de Carmichael. Con esta perspectiva consiguió una caracterización muy natural de estos números, derivando el problema de la búsqueda de números de Carmichael al estudio de lo que él mismo llamó *"una nueva función aritmética"*. Los enunciados siguientes suponen un análisis algo más moderno al que hizo Carmichael [Car10] en su artículo de 1910.

Definición 3.2.1 (Función de Carmichael)**.** Se denomina función de Carmichael a la aplicación $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ tal que

$$\lambda(n) = \text{mín}\{s \in \mathbb{N} : a^s \equiv 1 \pmod{n},\ \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}\ .$$

Observación 3.2.2. La función de Carmichael está bien definida gracias al Teorema 2.1.4, la Proposición 2.2.14 o el teorema de Lagrange.

El siguiente es un resultado clásico de la Teoría de Grupos que resultará útil para caracterizar la función de Carmichael.

Proposición 3.2.3. Sea $p > 2$ un primo y k un entero positivo. El grupo de unidades $(\mathbb{Z}/p^k\mathbb{Z})^*$ es cíclico.

Demostración. Si $k = 1$, el resultado es cierto por el Corolario 2.2.18.

Supongamos que $k > 1$. El orden de $(\mathbb{Z}/p^k\mathbb{Z})^*$ es $\varphi(p^k) = p^{k-1}(p-1)$. Como $\mathbb{F}_p$ es cíclico, podemos tomar un elemento generador g. Por una parte, el orden de g en $(\mathbb{Z}/p^k\mathbb{Z})^*$ es divisible por $p-1$ (el orden en $\mathbb{F}_p$ es exactamente $p-1$). Además, el teorema de Lagrange garantiza que además su orden divide al del grupo, $p^{k-1}(p-1)$. En consecuencia, el orden de g en $(\mathbb{Z}/p^k\mathbb{Z})^*$ debe ser de la forma $p^i(p-1)$ para algún $0 \leq i \leq k-1$, y el elemento g^{p^i} tiene orden $p-1$.

Veamos ahora que el elemento $1+p$ tiene orden p^{k-1} en $(\mathbb{Z}/p^k\mathbb{Z})^*$. Basta con observar que $(1+p)^{p^{k-2}} \equiv 1 \pmod{p^{k-1}}$ pero $(1+p)^{p^{k-2}} \not\equiv 1 \pmod{p^k}$.

- Es fácil comprobar que $(1+p)^p = \sum_{j=0}^{p} \binom{p}{j} p^j \equiv 1 \pmod{p^2}$ y que $(1+p)^p \equiv 1+p^2 \pmod{p^3}$, pues $p \mid \binom{p}{j}$ para todo $0 < j < p$.

- Sea $s > 1$. Supongamos que $(1+p)^{p^s} \equiv 1 + bp^{s+1} \pmod{p^{s+2}}$, con $0 < b < p$, y tratemos de probar que $(1+p)^{p^{s+1}} \equiv 1 + cp^{s+2} \pmod{p^{s+3}}$, con $0 < c < p$.

  El hecho de $(1+p)^{p^s} \equiv 1 + bp^{s+1} \pmod{p^{s+2}}$ implica que $(1+p)^{p^s} \equiv 1 + bp^{s+1} + dp^{s+2} = 1 + p^{s+1}(b+dp) \pmod{p^{s+3}}$, para algún $0 \leq d < p$. Podemos reescribir $b + dp = e$, donde además $e \equiv b \pmod{p}$ resultando que $(e, p) = 1$. Aplicando de nuevo el teorema del binomio, se encuentra

$$(1+p)^{p^{s+1}} = ((1+p)^{p^s})^p \equiv (1+ep^{s+1})^p = \sum_{j=0}^{p} \binom{p}{j} e^j p^{j(s+1)} \equiv 1+e^2p^{s+2} \pmod{p^{s+3}}\ .$$

Escogiendo $c = e^2 \pmod{p}$ se obtiene el resultado, de modo que el orden de $1+p$ en $(\mathbb{Z}/p^k\mathbb{Z})^*$ es p^{k-1}.

Considerando ahora el elemento $u = g^{p^i}(1+p)$, como $(p^{k-1}, p-1) = 1$, su orden debe ser $p^{k-1}(p-1) = \varphi(p^k)$. En consecuencia, $(\mathbb{Z}/p^k\mathbb{Z})^*$ es cíclico.

□

Observación 3.2.4. La razón por la que la demostración de la Proposición 2.8 no es válida para el caso $p = 2$ es que para asegurar $(1+p)^p \equiv 1+p^2 \pmod{p^3}$ se usa que $p|\binom{p}{j}$ para todo $j \geq 2$. En el caso $p = 2$ se tiene $\binom{2}{2} = 1$, siendo falso que $2^3|\binom{2}{2}2^2$. Sin embargo, se puede hacer una ligera modificación del segundo punto de la demostración anterior para obtener un resultado análogo para el orden de los elementos en el caso $p = 2$.

Es sencillo cerciorarse de que los grupos $(\mathbb{Z}/2\mathbb{Z})^*$ y $(\mathbb{Z}/4\mathbb{Z})^*$ son cíclicos, de modo que $\lambda(2^k) = \varphi(2^k)$ si $k = 1, 2$. Sin embargo, el máximo orden de cualquier elemento en $(\mathbb{Z}/8\mathbb{Z})^*$ es 2, resultando que no es cíclico y que además $\lambda(2^3) = 2$. Supongamos que $k > 3$ y veamos que el elemento $1 + 2 = 3$ tiene orden 2^{k-2} en $(\mathbb{Z}/2^k\mathbb{Z})^*$. Basta con observar que $3^{2^{k-3}} \equiv 1 \pmod{2^{k-1}}$ pero $3^{2^{k-3}} \not\equiv 1 \pmod{2^k}$. Reconstruimos la prueba de la Proposición 3.2.3 bajo nuestra nuevo hipótesis.

- Para $s = 4$ se tiene que $3^{2^{s-3}} = 3^2 \equiv 1 \pmod{2^{s-1} = 2^3}$ y $3^2 \equiv 1+2^3 \pmod{2^s = 2^4}$.
- Sea $s > 4$. Supuesto que $3^{2^{s-3}} \equiv 1 + 2^{s-1} \pmod{2^s}$, veamos que $3^{2^{s-2}} \equiv 1 + 2^s \pmod{2^{s+1}}$. El hecho de que $3^{2^{s-3}} \equiv 1+2^{s-1} \pmod{2^s}$ hace que $3^{2^{s-3}} \equiv 1+2^{s-1}+b2^s \pmod{2^{s+1}}$, siendo $b = 0, 1$. En cualquier caso, escribiendo $c = 1 + 2b$ se tiene que $3^{2^{s-3}} \equiv 1 + c2^{s-1} \pmod{2^{s+1}}$. Se sigue que

$$3^{2^{s-2}} = (3^{2^{s-3}})^2 \equiv (1 + c2^{s-1})^2 \equiv 1 + c2^s \pmod{2^{s+1}} .$$

Así que el orden de 3 en $(\mathbb{Z}/2^k\mathbb{Z})^*$ es 2^{k-2}. Por otra parte, dado $k > 2$ el teorema de Eüler garantiza que

$$X^{\varphi(2^k)} - 1 = X^{2^{k-1}} - 1 = (X^{2^{k-2}} - 1)(X^{2^{k-2}} + 1) \equiv 0 \pmod{2^k} .$$

Supongamos que existe alguna solución para la congruencia $X^{2^{k-2}} + 1 \equiv 0 \pmod{2^k}$. En ese caso, también existe solución para $X^{2^{k-2}} + 1 \equiv 0 \pmod{2^{k-1}}$, pero aplicando de nuevo el teorema de Eüler se encuentra

$$X^{2^{k-2}} + 1 = X^{2^{k-2}} - 1 + 2 \equiv 2 \not\equiv 0 \pmod{2^{k-1}} ,$$

de modo que no existe solución para la primera. Así pues, se tiene que $a \in (\mathbb{Z}/2^k\mathbb{Z})^*$ es una solución de $X^{2^{k-1}} - 1 \equiv 0 \pmod{2^k}$ si, y solamente si, lo es también de $X^{2^{k-2}} - 1 \equiv 0 \pmod{2^k}$. Por todo ello, el 3 es un elemento de orden máximo en $(\mathbb{Z}/2^k\mathbb{Z})^*$. En consecuencia, debe ser $\lambda(2^k) = \varphi(2^k)/2 = 2^{k-2}$, para $k > 2$.

La siguiente proposición determina de forma explícita los valores de la función de Carmichael.

Proposición 3.2.5. Si $n = p^\alpha$,

$$\lambda(n) = \begin{cases} \varphi(n) \text{ si } p \neq 2 \text{ o } \alpha \leq 2 \\ \frac{1}{2}\varphi(n) \text{ si } p = 2 \text{ y } \alpha > 2 \end{cases} .$$

Por otra parte, si $n = \prod_{i=1}^k p_i^{\alpha_i}$ es la factorización de n,

$$\lambda(n) = \text{mcm}(\lambda(p_i^{\alpha_i}) : 1 \leq i \leq k) .$$

Demostración. Resulta trivial que $\lambda(1) = 1$. También es claro por la Proposición 3.2.3 y la Observación 3.2.4 que, si p es primo y α un natural, $\lambda(p^\alpha) = \varphi(p^\alpha)$ si $p \neq 2$ o $\alpha \leq 2$, mientras que $\lambda(p^\alpha) = \varphi(p^\alpha)/2$ en otro caso.

Supongamos ahora que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Por el teorema chino de los restos, dado $(\mathbb{Z}/n\mathbb{Z})^*$ se tiene que

$$a^{\xi} \equiv 1 \pmod{n}$$

si, y sólo si

$$a^{\xi} \equiv 1 \pmod{p_i^{\alpha_i}}$$

para todo $1 \leq i \leq k$. Dado ξ satisfaciendo esta última condición, debe ser $\lambda(p^{\alpha_i}) \leq \xi$. Aplicando la división euclídea, se encuentra que $\xi = \lambda(p^{\alpha_i})q + r$, con q, r naturales y $1 \leq r < \lambda(p^{\alpha_i})$. Entonces

$$a^{\xi} = a^{\lambda(p^{\alpha_i})q+r} = a^{\lambda(p^{\alpha_i})q}a^r = (a^{\lambda(p^{\alpha_i})})^q a^r \equiv a^r \equiv 1 \pmod{p_i^{\alpha}} ,$$

y como $\lambda(p^{\alpha_i})$ es el mínimo exponente positivo con esa propiedad, debe ser $r = 0$. Por lo tanto, $\lambda(p_i^{\alpha_i})|\xi$ para cada $0 \leq i \leq k$, resultando que el menor ξ posible es $\lambda(n) = \text{mcm}(\lambda(p_i^{\alpha_i}) : 1 \leq i \leq k)$.

□

El teorema siguiente es la caracterización que Carmichael aportó de los números que llevan su nombre, publicada en 1912, dos años después del artículo en que presentó su función.

Teorema 3.2.6. *Sea n un entero positivo. El entero n es un número de Carmichael si, y sólo si, n es compuesto y $n \equiv 1 \pmod{\lambda(n)}$.*

Demostración. Por ser n es un número de Carmichael es compuesto y se tiene que para todo $a \in (\mathbb{Z}/n\mathbb{Z})^*$

$$a^{n-1} \equiv 1 \pmod{n} .$$

Como $\lambda(n) = \text{mín}\{s \in \mathbb{N} : a^s \equiv 1 \pmod{n}, \forall a \in (\mathbb{Z}/n\mathbb{Z})^*\}$, debe ser necesariamente $n - 1 \equiv 0 \pmod{\lambda(n)}$.

Del otro lado, sea n compuesto y tal que $n - 1 \equiv 0 \pmod{\lambda(n)}$. Entonces

$$a^{\lambda(n)} \equiv 1 \pmod{n} ,$$

y puesto que existe un entero q tal que $n - 1 = \lambda(n)q$

$$a^{n-1} = a^{\lambda(n)q} = (a^{\lambda(n)})^q \equiv 1 \pmod{n} ,$$

resultando que n es un número de Carmichael. □

3.3. Propiedades elementales de los números de Carmichael

En esta sección enunciamos algunas características básicas propias de los números de Carmichael. Éstas responden a las peculiaridades que presentan los números recogidos la Tabla 3.1, y algunas van más allá de lo que podría intuirse solamente a partir de la tabla. Terminaremos el capítulo desarrollando la reescritura que Paul Erdös realizó del criterio de Korselt, y explicando cómo ésta puede aprovecharse para demostrar algún resultado interesante acerca de la forma de los números de Carmichael.

Los siguientes teoremas [Wri12] restringen la factorización de un número de Carmichael.

Teorema 3.3.1. *Todo número de Carmichael n es impar, tiene al menos tres factores primos y todos sus divisores primos son menores que $\sqrt{n}$.*

Demostración. Comencemos viendo que n debe ser impar. Es claro que $(n, n-1) = 1$, de modo que $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \pmod{n}$ por ser n un número de Carmichael. Como $n > 2$ se tiene que $-1 \not\equiv 1 \pmod{n}$, y se sigue que $(-1)^{n-1} = 1$. En consecuencia, debe ser $n-1$ par y n impar.

Veamos ahora que n tiene al menos tres factores primos. Consideremos p un divisor primo de n. Se encuentra que

$$\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+n/p-1}{p-1} = \frac{n}{p} + \frac{n/p-1}{p-1} \ ,$$

de modo que $n/p - 1 \equiv 0 \pmod{p-1}$. Por ello, se tiene necesariamente que $p \leq n/p$. Además, la desigualdad debe ser estricta ya que en caso de alcanzarse la igualdad sería $n = p^2$, que no es posible por el Teorema 3.1.2. Por lo tanto $p^2 < n$, o equivalentemente $p < \sqrt{n}$.

Supongamos ahora que $n = pq$, con p, q primos. Debe tenerse que $p, q < \sqrt{n}$, pero en ese caso $n = pq < n$, llegándose a un absurdo. En conclusión, n debe tener más de dos factores primos. □

Proposición 3.3.2. Sea n un número de Carmichael. Si p, q son dos divisores primos de n, entonces $p \not\equiv 1 \pmod{q}$.

Demostración. Por el criterio de Korselt se tiene $n - 1 \equiv 0 \pmod{p-1}$. Esto supone que $n - 1 \equiv 0 \pmod{q}$, en contra de que $n - 1 \equiv 0 \pmod{q-1}$. Por ello, debe ser $p \not\equiv 1 \pmod{q}$. □

El siguiente es otro teorema interesante acerca de la forma de los números de Carmichael. Fue proporcionado por H. J. A. Duparc [Dup52] en el año 1952, como una generalización de un resultado anterior que N. G. W. H. Beeger [Bee50] aportó en 1950.

Teorema 3.3.3. *Sea $n = mpq$ un número de Carmichael, donde $q > p$ son primos. Entonces, se tiene que $p < 2m^2$ y $q < m^3$.*

Demostración. Por el criterio de Korselt, se verifica que

$$n = mpq \equiv mp \equiv 1 \pmod{q-1} \quad , \quad n \equiv mq \equiv 1 \pmod{p-1} \ .$$

Se definen los números naturales

$$V := \frac{mp-1}{q-1} \quad \text{y} \quad W := \frac{mq-1}{p-1} \ ,$$

que satisfacen $1 \leq V < m < W$. No es difícil ver

$$W(p-1) = mq - 1 = m(q-1) + m - 1 = m\left(\frac{mp-1}{V}\right) + m - 1 = m\left(\frac{mp-1}{V} + 1\right) - 1 \ .$$

En particular,

$$VW(p-1) = m^2p - m + mV - V = m^2(p-1) + m^2 - m + mV - V \ ,$$

de modo que

$$(VW - m^2)(p-1) = m^2 - m + mV - V = (m-1)(m+V) > 0 \ . \tag{3.1}$$

De nuevo, vuelve a ser fácil comprobar que $VW > m^2$. En consecuencia, de la Ecuación (3.1) se sigue que

$$(p-1) < (m-1)(m+V) < m^2 + m(V-1) \ , \tag{3.2}$$

y dado que $V < m$ se cumple que $p < 2m^2$. Por otra parte, de la Ecuación (3.2) se obtiene

$$q - 1 = \frac{mp-1}{V} < \frac{m^3 + m^2(V-1)}{V} < m^3 \ ,$$

resultando que $q < m^3$, lo que concluye la demostración. □

Corolario 3.3.4. *Sea I un conjunto finito y $\{p_i : i \in I\}$ una familia de primos distintos. El conjunto de los números de Carmichael de la forma*

$$n = qr \prod_{i \in I} p_i \ ,$$

donde q, r son dos primos distintos no pertenecientes a la familia, es finito.

Demostración. Supongamos que $r > q$. Basta con llamar $m = \prod_{i \in I} p_i$ para ver que, por el Teorema 3.3.3, se cumple que $q < 2m^2$ y $r < m^3$. Se sigue que la cantidad de números de Carmichael de esta forma está acotada superiormente por $2m^5$. □

En la Tabla 3.2 se recogen todos los pares de primos (p, q) que, fijado m, dan lugar a un número de Carmichael $n = mpq$. De acuerdo con el Corolario 3.3.4, el conjunto de pares para cada valor de m es finito.

m	3	5	7	11	13	15	21
(p,q)	(11,17)	(13,17)	(13,19)	(3,17)	(5,17)	(47,89)	-
		(13,29)	(13,31)		(7,31)		
		(17,29)	(19,67)		(37,61)		
			(23,41)		(37,97)		
			(31,73)		(37,241)		
			(73,103)		(47,89)		
					(61,397)		
					(97,421)		

Tabla 3.2: Cálculo de los números de Carmichael de la forma $n = mpq$, para $m = 3, 5, 7, 11, 13, 15, 21$. En efecto, solo hay una cantidad finita de ellos y está acotada por $2m^5$.

A fin de encontrar otras peculiaridades en la forma de los números de Carmichael es conveniente dar un paso atrás y analizar una versión alternativa del criterio de Korselt. La función que ahora definimos es necesaria en esta nueva formulación, y será fundamental para desarrollar muchos de los resultados incluídos en lo que resta de este trabajo (en especial el Capítulo 5),

Teorema 3.3.5. *Sea $n = \prod_{i=1}^{k} p_i$ un entero compuesto y $L(n) = \text{mcm}(p_i - 1 : 1 \leq i \leq k)$. Entonces, n es un número de Carmichael si, y solo si, $n \equiv 1 \pmod{L(n)}$.*

Demostración. Para comprobar que ambos resultados son equivalentes, basta con observar que $n \equiv 1 \pmod{L(n)}$ implica $n \equiv 1 \pmod{p-1}$ para todo divisor primo p de n y viceversa. □

El interés de esta reformulación fue encontrado primeramente por Erdös [Erd56], quien consideró oportuno estudiar enteros L' con una cantidad relativamente grande de divisores. Si un número suficiente de estos divisores son de la forma $p-1$ para algún primo, sería razonable que existieran subconjuntos $\{p_i : 1 \leq i \leq s\}$ de los mismos tales que $n = p_1 p_2 \dots p_s \equiv 1 \pmod{L'}$, en cuyo caso por el Teorema 3.3.5 el número n sería de Carmichael. Con esta perspectiva Erdös aportó una cota superior para la función contador de los números de Carmichael $C(x)$ (i.e. los números de Carmichael menores o iguales que x), que demostramos en la Sección 5.1 del Capítulo 5. Aportó también un argumento heurístico para deducir una cota inferior con límite infinito para los números de Carmichael. Sin embargo no fue capaz de proporcionar una demostración rigurosa. Sí lo lograron R. Alford, A. Granville y C. Pomerance [AGP94], quienes tomaron el testigo de la visión de Erdos y consiguieron demostrar en 1994 la infinitud de los números de Carmichael. Discutiremos sus resultados en la Sección 5.2 del Capítulo 5.

Los siguientes resultados, tomados de [Wri12], relacionan la forma de los números de Carmichael con la función L.

Teorema 3.3.6. *Sea $n = \prod_{j=1}^{k} p_j$ un número de Carmichael. Escribamos $p_i = 2^{s_i} D_i + 1$, con D_i impar para cada $1 \leq i \leq k$, de forma que $s_1 \leq \ldots \leq s_k$. Entonces, si $2^{s_1+1} | L(n)$ se tiene que $s_1 = s_2$.*

Demostración. Se procede por reducción al absurdo. Supongamos que $2^{s_1+1} | L(n)$ y $s_1 < s_2$. Entonces,

$$n = \prod_{j=1}^{k} p_j = \prod_{i=1}^{k} (2^{s_i} D_i + 1) \equiv 2^{s_1} D_1 + 1 \pmod{2^{s_1+1}} .$$

Por otra parte, como n es de Carmichael y $2^{s_1+1} | L(n)$, el Teorema 3.3.5 garantiza que

$$n \equiv 1 \pmod{2^{s_1+1}} .$$

Así que

$$2^{s_1} D_1 + 1 \equiv 1 \pmod{2^{s_1+1}},$$

obligando a que D_1 sea par, que no es cierto. En consecuencia, debe ser $s_1 = s_2$. □

Teorema 3.3.7. *Si $n = \prod_{j=1}^{k} p_i$ es un número de Carmichael, entonces $L(n)$ no es de la forma 2^s. En consecuencia, ningún número de Carmichael es de la forma $2^u + 1$.*

Demostración. Procedemos por reducción al absurdo. Supongamos que $L(n) = 2^s$ para algún s. Recordando que $L(n) = \text{mcm}(p_j - 1 : 1 \leq j \leq k)$, puede escribirse $p_i = 2^{v_i} + 1$ para cada $1 \leq i \leq k$ con $0 \leq v_i \leq s$ y $v_1 < \ldots < v_k$. Por ello, $2^{v_1+1} | 2^{v_l} | L(n)$ para todo $2 \leq l \leq k$, en contra del Teorema 3.3.6, de modo que no es posible que $L(n) = 2^s$. Como los únicos divisores de una potencia de 2 son otras potencias de 2 con exponente menor o igual, no es posible que exista ningún número de Carmichael de la forma $2^u + 1$. □

Corolario 3.3.8. *Ningún número de Fermat es un número de Carmichael.*

Existen más resultados que restringen la forma de los números de Carmichael estudiando el valor de L. En particular, en el mismo trabajo [Wri12] se obtiene la siguiente relación: si la conjetura de los primos de Fermat es cierta (i.e. existe solo un número finito de ellos), el conjunto de números de Carmichael con $L = 2^k p$, siendo p primo, es finito. Sin embargo, el amplio conjunto de resultados relacionados con los números de Carmichael hace que en este trabajo se opte por evitar resultados demasiado específicos, ya que esto supondría dejar de lado otras corrientes de estudio acerca de estos números que son fundamentales.

Capítulo 4

Construcción de números de Carmichael

En este capítulo abordamos el problema de generar números de Carmichael. Como comentamos al comienzo del Capítulo 3, fue Carmichael quien proporcionó los primeros ejemplos de los números que llevan su nombre, valiéndose de la caracterización del Teorema 3.2.6. Su aportación se limitó a 14 ejemplos con exactamente 3 factores primos, entre los que estaban $24655 = 5 \cdot 17 \cdot 29$ y $399001 = 31 \cdot 61 \cdot 211$, y solamente uno con 4 factores primos, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$. Algunos años después de la publicación de los resultados de Carmichael, otros matemáticos lograron aumentar la lista de números conocidos. Entre ellos estaba Paul Poulet, quien enumeró todos los pseudoprimos para la base 2 (i.e. números de Poulet) por debajo de 10^8 [Pou38], entre los que se encontraban algunos números de Carmichael que habían pasado inadvertidos hasta la fecha. A modo de anécdota, Poulet se equivocó en algunos de los números que incluyó como pseudoprimos para la bases 2.

Uno de los trabajos más importantes en relación a la construcción de números de Carmichael vino de la mano de Jack Chernick. En su trabajo [Che39] desarrolló la noción de forma universal que estudiaremos con detalle en este capítulo, y con ella consiguió generar más números de Carmichael que cualquier otro autor anterior. Más aún, la mayoría de los algoritmos modernos para generar números de Carmichael son modificaciones de las formas universales de Chernick. Además, las ideas de Chernick están íntimamente relacionadas con uno de los problemas abiertos más reseñables en teoría de números: la conjetura de Dickson. En efecto, comprobaremos que si ésta es cierta entonces los métodos de Chernick pueden emplearse para construir infinitos números de Carmichael. Aunque, como ya hemos anticipado, la demostración de la existencia de infinitos números de Carmichael se completó aplicando otras técnicas que no están relacionadas con la conjetura de Dickson. En caso de que ésta fuera cierta, podrían calcularse sucesiones de números de Carmichael arbitrariamente largas, y se obtendría además una demostración "constructiva" (aunque también tendría serias limitaciones) de la existencia de infinitos números de Carmichael con una cantidad fija de factores primos. Pese a que la demostración de esta conjetura parece fuera de alcance con los métodos actuales, se conoce un caso particular en que sí es cierta, y algunos resultados parciales entre los que destaca el reciente teorema de Maynard-Tao. Lógicamente, en este capítulo enunciamos y discutimos todos los resultados mencionados en este párrafo.

En este capítulo nos centramos en la construcción de números de Carmichael a través de formas universales. Veremos cómo deducir fórmulas para generar estos números y cómo obtener nuevos números de Carmichael a partir de otros añadiendo algún factor primo.

4.1. Formas universales y la conjetura de Dickson

El siguiente resultado, debido a Chernick [Che39], recoge la idea subyaciente a las formas universales.

Teorema 4.1.1. *Sea n un número de Carmichael con exactamente tres divisores primos. Entonces, $n = (2r_1h + 1)(2r_2h + 1)(2r_3h + 1)$, con r_1, r_2, r_3 coprimos dos a dos.*

Demostración. Sea $n = p_1p_2p_3$, con p_i primo. Llamando $u = (p_1 - 1, p_2 - 1, p_3 - 1)$[1], puede escribirse $p_i = r_iu + 1$ con $(r_1, r_2, r_3) = 1$. Por el criterio de Korselt, para cada $i = 1, 2, 3$, se encuentra

$$(r_1u + 1)(r_2u + 1)(r_3u + 1) \equiv 1 \pmod{r_iu} ,$$

de donde se deduce que

$$u(r_1r_2 + r_1r_3 + r_2r_3) + r_1 + r_2 + r_3 \equiv 0 \pmod{r_i} . \tag{4.1}$$

De la congruencia anterior se extrae que si $(r_i, r_j) \neq 1$ para $1 \leq i, j \leq 3$, $i \neq j$, se tiene entonces que $(r_1, r_2, r_3) \neq 1$. Como esto no es posible, r_1, r_2, r_3 son coprimos dos a dos. Por otra partep_1, p_2, p_3 son impares, así que u debe ser par. Por tanto puede escribirse $u = 2h$ y el resultado queda demostrado. □

Observación 4.1.2. Hay que notar que el recíproco del teorema anterior no es cierto. Por ejemplo, escogiendo $(r_1, r_2, r_3) = (1, 2, 3)$ se obtiene $n = (2 + 1)(4 + 1)(6 + 1) = 105$, que no es de Carmichael porque $105 \equiv 9 \not\equiv 1 \pmod{L(105)}$, siendo $L(105) = 12$.

Volviendo sobre la demostración anterior, las tres congruencias englobadas en (4.1) pueden reescribirse de forma compacta como

$$u(r_1r_2 + r_1r_3 + r_2r_3) + r_1 + r_2 + r_3 \equiv 0 \pmod{r_1r_2r_3} .$$

Además, el teorema chino garantiza que el orden de $(r_1r_2 + r_1r_3 + r_2r_3) \pmod{r_1r_2r_3}$ es divisor de $\varphi(r_1)\varphi(r_2)\varphi(r_3)$. Llamando $e = \varphi(r_1)\varphi(r_2)\varphi(r_3) - 1$, la solución general para u en la congruencia (4.1) es

$$u(M) = Mr_1r_2r_3 - (r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3)^e . \tag{4.2}$$

con M entero. De este modo, escogiendo tres enteros positivos r_1, r_2, r_3, coprimos dos a dos, se obtiene una familia numerable $\{(y(M) = (u(M)r_1 + 1)(u(M)r_2 + 1)(u(M)r_3 + 1) : M \in \mathbb{N}\}$ de enteros tales que $y(M) \equiv 1 \pmod{r_iM}$ para cada $1 \leq i \leq 3$. En consecuencia, si los factores $(u(M)r_i + 1)$ son simultáneamente primos, cualquier elemento de la sucesión $y(M)$ satisfará el criterio de Korselt y por ende será un número de Carmichael. Éste fue históricamente el primer indicio fuerte a favor de la existencia de infinitos números de Carmichael, y es aquí donde radica la conexión con una cuestión abierta en teoría de números. En 1904, L. E. Dickson [Dic04] planteó la siguiente conjetura.

Conjetura 4.1.3. Existen familias $\mathcal{H}(n) = \{g_in + h_i\}_{i=1}^k$ con g_i, h_i naturales tales que para infinitos valores de n todos los elementos de $\mathcal{H}(n)$ son primos.

[1]Mantenemos la notación habitual de máximo común divisor aunque se trate de más de dos números. Es decir, $(p_1 - 1, p_2 - 1, p_3 - 1) = \text{mcd}\{p_1 - 1, p_2 - 1, p_3 - 1\}$

A día de hoy sigue sin conocerse una respuesta acerca de la veracidad del enunciado anterior, pero no es complicado comprobar que en caso de ser cierta sería posible emplear expresiones similares a $y(M) = (u(M)r_1 + 1)(u(M)r_2 + 1)(u(M)r_3 + 1)$ para construir sucesiones infinitas de números de Carmichael. Sí se conoce que el enunciado es cierto para el caso $k = 1$, como afirma el siguiente resultado conocido como teorema de Dirichlet para progresiones aritméticas.

Teorema 4.1.4 (Dirichlet, 1837)**.** *Si g,h son dos enteros con* $(g, h) = 1$*, entonces la sucesión* $(gn+h)_{i=1}^{\infty}$ *contiene infinitos números primos. Equivalentemente, existen infinitos números primos congruentes a* $h \pmod{g}$*.*

Comparando los enunciados de la conjetura de Dickson y el teorema de Dirichlet observamos que, mientras que el segundo impone la restricción de que $(g, h) = 1$, en el primero no se concreta nada sobre la relación entre g y h. Existen familias $\{g_i n + h_i\}_{i=1}^{k}$ para las que podemos garantizar que la condición de la conjetura de Dickson no se cumple. Este es el caso, por ejemplo, de la familia $\{g_i n + g_i\}_{i=1}^{k}$ para cualesquiera $g_i > 1$. La siguiente definición permite concretar qué familias de polinomios lineales $\{g_i n + h_i\}_{i=1}^{k}$ están en condiciones de estar formadas enteramente por primos para infinitos valores de n.

Definición 4.1.5 (k-tupla admisible)**.** Sea la familia $\mathcal{H}(n) = \{g_i n + h_i\}_{i=1}^{k}$ con g_i, h_i naturales. Diremos que $\mathcal{H}$ es admisible si, para todo primo p, existe algún entero n tal que

$$p \nmid \prod_{i=1}^{k} (g_i n + h_i) \ .$$

Una versión alternativa de la conjetura de Dickson es que toda $k-tupla$ admisible esta compuesta enteramente por números primos para infinitos valores de n. Pese a que esta última afirmación es más fuerte que el enunciado citado anteriormente (ya no hablamos de existencia si no de una familia de k-tuplas concreta), está respaldado por uno de los más recientes hitos en el campo de la teoría de números. En el año 2013, los matemáticos James Maynard y Terrence Tao dedujeron de forma independiente[2] la siguiente aproximación a la conjetura de Dickson.

Teorema 4.1.6 (Maynard-Tao, 2013)**.** *Sea* $\mathcal{H}(n) = \{g_i n + h_i\}_{i=1}^{k}$ *una k-tupla admisible. Para todo* $m \geq 2$ *existe una constante positiva D tal que, si* $m > D \exp(8m)$*, entonces para infinitos valores de n al menos m de los elementos en* $\mathcal{H}$ *son primos* [3]*.*

Dando un paso atrás, el desarrollo motivado a raíz del teorema 4.1.1 puede generalizarse a expresiones con un número arbitrario de factores lineales. La siguiente definición presenta el concepto pionero de las formas universales, muy útiles en la construcción de números de Carmichael.

Definición 4.1.7. Sea $n \geq 3$ y $\mathcal{F} = \{(a_i, b_i) : 1 \leq i \leq n\}$ una familia de pares de números naturales con a_i par y b_i impar. Se llama forma universal asociada a $\mathcal{F}$ a todo polinomio

$$U_n(M) = \prod_{i=1}^{n} (a_i M + b_i)$$

que satisfaga $U_n(M) \equiv 1 \pmod{a_i M + b_i - 1}$, para cada $1 \leq i \leq n$, y para todo M entero.

[2] Aunque los dos llegaron a la misma conclusión, la cota que Maynard obtuvo era más fina que la de Tao.

[3] Recientes mejoras realizadas por los matemáticos involucrados en el proyecto POLYMATH han conseguido reducir la cota exponencial a $m > D \exp(4m)$ [Wri12].

El propósito de la definición anterior es simple: utilizar las formas universales como fórmulas con las que generar números de Carmichael. Por el criterio de Korselt, la única condición necesaria para que esto ocurra es que dado un n, todos los factores lineales que la componen sean simultáneamente primos. En la Tabla 4.1 se muestran algunas formas universales $U_3(M) = (u(M)r_1 + 1)(u(M)r_2 + 1)(u(M)r_3 + 1)$ para los casos más sencillos, calculados a partir de la relación (4.2).

(r_1, r_2, r_3)	u	U_3
(1,2,3)	$6M$	$(6M + 1)(12M + 1)(18M + 1)$
(1,2,5)	$10M + 6$	$(10M + 7)(20M + 13)(50M + 31)$
(1,3,4)	$12M + 4$	$(12M + 5)(36M + 13)(48M + 17)$
(1,4,5)	$20M + 10$	$(20M + 11)(80M + 41)(100M + 51)$
(2,3,5)	$30M + 20$	$(60M + 41)(90M + 61)(150M + 101)$
(3,4,5)	$60M + 24$	$(180M + 73)(240M + 97)(300M + 121)$
(1,3,8)	$24M + 12$	$(24M + 13)(72M + 37)(192M + 97)$
(1,5,8)	$40M + 2$	$(40M + 3)(200M + 11)(320M + 17)$
(2,5,9)	$90M + 38$	$(180M + 77)(450M + 191)(810M + 343)$

Tabla 4.1: Primeros ejemplos de U_3.

Cada una de las expresiones de la Tabla 4.1 puede utilizarse como una fórmula para generar números de Carmichael. De nuevo, si la conjetura de Dickson es cierta existirán múltiples formas universales capaces de generar infinitos números de Carmichael. La primera de todas, $U_3(M) = (6M+1)(12M+1)(18M+1)$, es especialmente común en la literatura. A todos los números de Carmichael que genera se les conoce como números de números de Chernick. En la Tabla 4.2 de la siguiente página se recogen los números de Carmichael generados a partir de ella, junto a los generados por $U_3(M) = (60M + 41)(90M + 61)(150M + 101)$, para $0 \leq M \leq 1000$. De igual manera pueden escogerse otras expresiones de la Tabla 4.1 y realizar el mismo cálculo para obtener nuevos números de Carmichael. Sin embargo, por razones de espacio, nos limitamos a mostrar exclusivamente estos dos casos. La cantidad de ejemplos recogidos en la Tabla 4.2 pone de manifiesto la utilidad de las formas universales en la generación de números de Carmichael, ya que se superan con creces los 14 que pudo aportar Carmichael.

4.2. Formas universales con más de 3 factores

En lo concerniente al cálculo de formas universales con más de tres factores lineales, puede probarse que si $n = \prod_{i=1}^{k} p_i$ es un número de Carmichael, entonces es posible reescribirlo como $n = \prod_{i=1}^{k}(r_i h+1)$, donde $r_1, r_2, \ldots, r_k$ son coprimos en conjuntos de $k-1$ elementos. Sin embargo, en caso de seguir el mismo camino que para $k = 3$, las congruencias a resolver son mucho más complejas. En general, denotando $S_j := S_j[r_1, r_2, \ldots, r_k]$ a la j-ésima función simétrica elemental, debería resolverse

$$\sum_{j=1}^{k-1} u^{j-1} S_j \equiv 0 \pmod{r_i} ,$$

ecuación que generaliza a (4.1). La dificultad creciente motiva la búsqueda de nuevos caminos hacia el cálculo de nuevos formas universales. El siguiente permite generar formas universales a partir de números de Carmichael ya conocidos.

$U_3 = (6M+1)(12M+1)(18M+1)$				$U_3 = (60M+41)(90M+61)(150+101)$			
M	$6M+1$	$12M+1$	$18M+1$	M	$60M+41$	$90M+61$	$150M+101$
1	7	13	19	0	41	61	101
6	37	73	109	1	101	151	251
35	211	421	631	4	281	421	701
45	271	541	811	7	461	691	1151
51	307	613	919	21	1301	1951	3251
55	331	661	991	24	1481	2221	3701
56	337	673	1009	31	1901	2851	4751
100	601	1201	1801	43	2621	3931	6551
121	727	1453	2179	46	2801	4201	7001
195	1171	2341	3511	70	4241	6361	10601
206	1237	2473	3709	99	5981	8971	14951
216	1297	2593	3889	108	6521	9781	16301
255	1531	3061	4591	109	6581	9871	16451
276	1657	3313	4969	112	6761	10141	16901
370	2221	4441	6661	154	9281	13921	23201
380	2281	4561	6841	158	9521	14281	23801
426	2557	5113	7669	176	10601	15901	26501
506	3037	6073	9109	213	12821	19231	32051
510	3061	6121	9181	218	13121	19681	32801
511	3067	6133	9199	234	14081	21121	35201
710	4261	8521	12781	238	14321	21481	35801
741	4447	8893	13339	267	16061	24091	40151
800	4801	9601	14401	273	16421	24631	41051
825	4951	9901	14851	311	18701	28051	46751
871	5227	10453	15679	319	19181	28771	47951
930	5581	11161	16741	337	20261	30391	50651
975	5851	11801	17551	381	22901	34351	57251
				515	30941	46411	77351
				518	31121	46681	77801
				519	31181	46771	77951
				528	31721	47581	79301
				540	32441	48661	81101
				658	39521	59281	98801
				680	40841	61261	102101
				689	41381	62071	103451
				704	42281	63421	105701
				736	44201	66301	110501
				739	44381	66571	110951
				752	45161	67741	112901
				781	46901	70351	117251
				837	50261	75391	125651
				889	53381	80071	133451

Tabla 4.2: Números de Carmichael generados a partir de las formas universales $U_3(M) = (6M+1)(12M+1)(18M+1)$, $U_3(M) = (60M+41)(90M+61)(150M+101)$, con $0 \leq M \leq 1000$.

Teorema 4.2.1. *Sea $n = \prod_{i=1}^{k} p_i$ un número de Carmichael. Denotemos*

$$u_1 = (p_1 - 1, p_2 - 1, \ldots, p_k - 1) \quad , \quad r_i = (p_i - 1)/u_1 \quad , \quad R = \text{mcm}(r_1, r_2, \ldots, r_k) \ .$$

Entonces, $U_k(M) = \prod_{i=1}^{k}(r_i RM + p_i)$ es una forma universal salvo que todos los r_i sean impares, en cuyo caso M debe sustituirse por $2M$.

Demostración. Por el criterio de Korselt,

$$n - 1 = \left(\prod_{i=1}^{k} p_i\right) - 1 = \prod_{i=1}^{k}(r_i u_1 + 1) - 1 \equiv 0 \pmod{p_j - 1 = r_j u_1} \ , \forall 1 \leq j \leq k$$

En consecuencia,

$$\prod_{i=1}^{k}(r_i u_1 + 1) - 1 \equiv 0 \pmod{r_j} \quad , \quad \prod_{i=1}^{k}(r_i u_1 + 1) - 1 \equiv 0 \pmod{u_1} \ ,$$

y como $(r_j, u_1) = 1$, podemos escribir

$$\left(\prod_{i=1}^{k}(r_i u_1 + 1) - 1\right)/u_1 \equiv 0 \pmod{R} \ .$$

Teniendo en cuenta que $\prod_{i=1}^{k}(r_i u + 1) - 1 \equiv 0 \pmod{u}$ para cualquier entero no nulo u, es claro que toda solución $u \equiv u_1 \pmod{R}$ también satisface la última congruencia. En particular, $u = MR + u_1$, y sustituyendo en la congruencia anterior se obtiene

$$\left(\prod_{i=1}^{k}(r_i MR + p_i) - 1\right)/(MR + u_1) \equiv 0 \pmod{R} \ .$$

o equivalentemente

$$\prod_{i=1}^{k}(r_i RM + p_i) \equiv 1 \pmod{R(MR + u_1)} \ .$$

Como $R \equiv 0 \pmod{r_j}$ para todo $0 \leq j \leq k$, la congruencia se sigue satisfaciendo $\pmod{r_j(MR + u_1)}$. Dado que $r_j(MR + u_1) = r_j MR + p_i - 1$, se satisface que $U_k \equiv 1 \pmod{a_i M + b_i - 1}$ para cada $1 \leq i \leq k$. Si se cumple r_i es par para algún $1 \leq i \leq k$, entonces también lo será R y U_n es una forma universal forma universal. Si por el contrario todos los r_i son impares, basta reemplazar M por $2M$ para que todos los coeficientes que multiplican a M sean pares, y U_n es una forma universal. □

En la Tabla 4.3 se recogen algunas formas universales generadas a partir de números de Carmichael y el Teorema 4.2.1. En los casos de $7 \cdot 13 \cdot 19$ y $16061 \cdot 24091 \cdot 40151$, que pertenecen a la Tabla 4.2, se obtienen los mismos coeficientes para la M que la forma con que se generaron.

n	U
$7 \cdot 13 \cdot 19$	$(6M+7)(12M+13)(18M+19)$
$7 \cdot 23 \cdot 31$	$(2 \cdot 495M+7)(2 \cdot 1815M+23)(2 \cdot 2475M+31)$
$16061 \cdot 24091 \cdot 40151$	$(60M+16061)(90M+24091)(150M+40151)$
$7 \cdot 11 \cdot 13 \cdot 101$	$(450M+7)(750M+11)(900M+13)(7500M+101)$
$13 \cdot 13 \cdot 19 \cdot 73$	$(12M+7)(24M+13)(36M+19)(144M+73)$

Tabla 4.3: Cálculo de las formas universales asociadas a algunos números de Carmichael, de acuerdo con el esquema propuesto en el Teorema 4.2.1.

En relación con el resultado anterior, el siguiente método permite el cálculo de nuevos números de Carmichael a partir de otros.

Teorema 4.2.2. *Sea $F_{n-1} = \prod_{i=1}^{n-1} p_i$ un número de Carmichael. Se denota $k = \text{mcm}(p_1 - 1, p_2 - 2, \ldots, p_{n-1} - 1)$ y $r = (F_{n-1} - 1)/k$. Entonces, si $p_n = kq + 1$ es un primo distinto a p_i para todo $1 \leq i \leq n-1$, donde $r \equiv 0 \pmod{q}$, $F_n := F_{n-1} \cdot p_n$ es un número de Carmichael.*

Demostración. Se verifica que $F_n \equiv F_{n-1} \cdot p_n \equiv F_{n-1} \equiv 1 \pmod{k}$, y como $k \equiv 0 \pmod{p_i - 1}$ para cada $1 \leq i \leq n-1$, la congruencia se sigue cumpliendo $\pmod{p_i - 1}$. Por otra parte, $F_n \equiv F_{n-1} \cdot p_n \equiv F_{n-1} \equiv 1 \pmod{p_n - 1}$, así que se satisface la condición del criterio de Korselt y F_n es un número de Carmichael. □

En la Tabla 4.2 se presentan algunos de los números de Carmichael que pueden contruirse, tal y como indica el Teorema 4.2.2, partiendo de los números de Carmichael $n_1 = 5 \cdot 17 \cdot 29 = 2465$, $n_2 = 7 \cdot 13 \cdot 31 = 2821$ y $n_3 = 7 \cdot 13 \cdot 19 = 1729$.

$5 \cdot 17 \cdot 29$	$7 \cdot 13 \cdot 31$	$7 \cdot 13 \cdot 19$
$5 \cdot 17 \cdot 29 \cdot 113$	$7 \cdot 13 \cdot 31 \cdot 61$	$7 \cdot 13 \cdot 19 \cdot 109$
$5 \cdot 17 \cdot 29 \cdot 113 \cdot 337$	$7 \cdot 13 \cdot 31 \cdot 61 \cdot 181$	$7 \cdot 13 \cdot 19 \cdot 109 \cdot 541$
$5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673$	$7 \cdot 13 \cdot 31 \cdot 61 \cdot 181 \cdot 541$	$7 \cdot 13 \cdot 19 \cdot 109 \cdot 541 \cdot 129061$

Tabla 4.4: Extensión de algunos números de Carmichael calculados previamente añadiendo más factores primos.

Resulta clara la complementariedad existente entre los Teoremas 4.2.1 y 4.2.2. El primero produce formas universales con las que deberían poderse generar nuevos números de Carmichael (aunque por supuesto depende de la validez de la conjetura de Dickson), mientras que el segundo aumenta el número de primos en la factorización de los anteriores para que de nuevo se puedan generar nuevas formas universales con el primer teorema.

Es importante destacar que el Teorema 4.2.2 es, de algún modo, generalizable a las formas universales U_n en las que los términos independientes de todos los factores lineales son 1. Si se omite la condición de primalidad de cada factor, el teorema puede aplicarse sobre formas universales para obtener nuevas expresiones. Con esta idea es posible garantizar la existencia de al menos una forma universal con un número arbitrariamente grande de factores lineales.

Teorema 4.2.3. *Existe una forma universal para cualquier $n \geq 4$.*

Demostración. Partiendo de $U_3 = (6M+1)(12M+1)(18M+1)$, se calculan nuevas formas universales añadiendo factores lineales. Aplicamos inducción sobre el número de factores

n, comenzando por comprobar que el enunciado es cierto para $n = 4$. Para ello, veamos que la expresión

$$U_4 = (6M + 1)(12M + 1)(18M + 1)(36M + 1)$$

es una forma universal. Ya conocemos que $U_3 = (6M + 1)(12M + 1)(18M + 1)$ lo es, y además $36M + 1 \equiv 1 \pmod{6M} \pmod{12M} \pmod{18M}$. Por ello, solo queda comprobar que $U_4 \equiv 1 \pmod{36M}$. En efecto

$$U_4 \equiv U_3 = 1 + M(6 + 12 + 18) + M^2(6 \cdot 12 + 6 \cdot 18 + 12 \cdot 18) + M^3 \cdot 6 \cdot 18 \cdot 36 \equiv 1 \pmod{36M}$$

y U_4 es una forma universal.

Tomando $n > 4$, suponemos que $U_k = (6M + 1)(12M + 1) \prod_{i=1}^{k-2}(2^i \cdot 9M + 1)$ es una forma universal en la variable N, donde $M = 2^{n-4}N$, para todo $k \leq n$. Comprobamos que el resultado sigue siendo válido para $n + 1$. Para ello, definimos

$$U_{n+1} = (6M + 1)(12M + 1) \prod_{i=1}^{n-1}(2^i \cdot 9M + 1) \ .$$

Teniendo en cuenta que U_n es una forma universal, $U_n \equiv 2^{n-1}9M + 1 \equiv 1 \pmod{6M}$, $\pmod{12M}$, $\pmod{2^j 9M}$, para todo $1 \leq j \leq n - 2$. Por ello U_{n+1} satisfará las mismas congruencias, y solo es necesario comprobar que

$$U_{n+1} \equiv U_n \equiv 1 \pmod{2^{n-1}9M} \tag{4.3}$$

para concluir que U_{n+1} es universal. Puede desarrollarse

$$U_{n+1} = 1 + M(6 + 12 + 18 + \ldots + 2^{n-2}9) + h[M]M^2,$$

donde $h[M]$ es un polinomio en la variable M. Observando que el término entre paréntesis de la identidad anterior es igual a $2^{n-1}9$, resulta que

$$h[M]M \equiv 0 \pmod{2^{n-1}9}$$

es equivalente a la congruencia (4.3). Sin embargo, teniendo en cuenta que $h[M] \equiv 0 \pmod{2^2 \cdot 3}$, puede escogerse $N_1 = 2N$ de forma que $M = 2^{n-4}N = 2^{n-3}N_1$ y se satisface la congruencia. Por ello, U_{n+1} es una forma universal en la variable N_1 y el resultado queda demostrado.abre una nueva vía en la generación de números de Carmichael □

En base al base al teorema anterior, es razonable pensar que pueden generalizarse otras formas universales para obtener nuevas expresiones con un número arbitrario de factores lineales. Este hecho parece útil, en la medida de que permite mantener la estrategia empleada hasta ahora de utilizar formas universales para generar números de Carmichael con una cantidad fija de factores primos. Sin embargo, desde un punto de vista práctico, no es viable emplear formas universales con demasiados factores. La razón es la dificultad intrínseca a que todos los polinomios lineales que componen la forma sean simultáneamente primos cuando se evalúan en un cierto entero. Además, como veremos en el Capítulo 4, está conjeturado que la densidad de los números de Carmichael con exactamente k factores primos disminuye a medida que crece k (puede comprobarse acudiendo a la Tabla 5.1 de la página 46, que hasta 10^{16} solamente hay 23 números de Carmichael con 10 factores primos), lo que hace aún menos probable que alguno de éstos números de Carmichael esté generado por alguna de las formas universales trabajadas.

Como hemos visto en este capítulo, las ideas de Chernick supusieron un fuerte impulso en lo concerniente al cálculo de números de Carmichael. Desde la publicación de su artículo en 1939, múltiples autores desarrollaron aún más sus ideas para generar largas listas de nuevos números de Carmichael. Entre ellos destaca M. Yorinaga [Yor78a] [Yor78b], quien dedicó dos artículos consecutivos a presentar sus cálculos. Otros, como D. Woods y J. Huenemann [WH82], diseñaron variantes a las técnicas de Chernick. La proposición siguiente recoge el procedimiento seguido por estos dos últimos autores.

Proposición 4.2.4. Sea $n = (6M+1)(12M+1)(18M+1)$ un número de Carmichael. Si F es un divisor de $36M^2+11M+1$ tal que $36FM+1$ es primo, entonces $C = (6M+1)(12M+1)(18M+1)(36FM+1) = n(36FM+1)$ es un número de Carmichael.

Demostración. Desarrollando n, se encuentra

$$n = (6M+1)(12M+1)(18M+1) = 36M(36M^2+11M+1)+1 \ .$$

Por tanto, si F es un divisor de $36M^2+11M+1$, $36FM$ es un divisor de $n-1$. Además, $C = n(36FM+1) = 36FMn + n \equiv 1 \pmod{6M} \pmod{12M} \pmod{18M}$. En consecuencia, si $36FM+1$ es primo, el criterio de Korselt garantiza que C es de Carmichael. □

Aprovechando cálculos anteriores, podemos reutilizar los números de la Tabla 4.2 para deducir otros nuevos en base a la proposición anterior. En la Tabla 4.5 se presentan todos los números de Carmichael obtenibles a partir de la Proposición 4.2.4, para los primeros números de Chernick.

M	$U_3(M)$	$36M^2+11M+1$	F	$36FM+1$
1	$7 \cdot 13 \cdot 19$	48	1	37
			2	73
			3	109
			12	433
			16	577
35	$211 \cdot 421 \cdot 631$	44486	2	2521
			13	16381
			29	36541
			754	950041
			1534	1932841
			1711	2155861
			22243	28026181
45	$271 \cdot 541 \cdot 811$	73396	1	1621
			4	6481
			59	95581
			118	191161
			311	503821

Tabla 4.5: Cálculo de los todos los números de Carmichael susceptibles de obtenerse siguiendo la estrategia de la proposición 4.2.4, para los primeros números de Chernick.

Capítulo 5

Densidad de los números de Carmichael

Hasta ahora, nos hemos limitado a emplear herramientas puramente algebraicas en nuestro estudio de los números de Carmichael. Sin embargo, hay ciertas preguntas que parecen difíciles de responder con estos métodos. En efecto, pese a la experiencia ganada hasta este punto del trabajo, segumos sin tener respuesta para las siguientes cuestiones: ¿Cuántos números de Carmichael existen hasta una cierta cantidad x?¿Existen infinitos números de Carmichael? En caso de que la respuesta a la pregunta anterior sea afirmativa, ¿con qué frecuencia encontramos números de Carmichael entre los números naturales? En otras palabras, ¿podemos comparar el crecimiento de los números de Carmichael con alguna función conocida? Desde luego estas preguntas son completamente razonables, y no responderlas significaría dejar un hueco importante en nuestro análisis sobre los números de Carmichael. Sin embago, la respuesta a alguna de ellas no es en absoluto sencilla, y no se conocía hasta hace apenas dos décadas. Otras, sorprendentemente, solo tienen una respuesta parcial.

Todas las cuestiones anteriores están relacionadas con la densidad de los números de Carmichael. Por esta razón, a fin de abordarlas, es conveniente definir una función análoga a $\pi(x)$ (la función contador de primos) para los números de Carmichael. En lo sucesivo, $C(x)$ denotará la función contador de los números de Carmichael inferiores a x,

$$C(x) = |\{n \leq x : n \text{ es de Carmichael}\}| \ . \tag{5.1}$$

No es difícil reescribir las preguntas anteriormente planteadas en términos de la función C. En concreto, el problema de estudiar la frecuencia con la que aparecen los números de Carmichael puede expresarse como: *¿Existe alguna función real y de variable real (analítica, o al menos continua) g tal que*

$$\lim_{x\to\infty} \frac{C(x)}{g(x)} = 1 \ ?$$

Si es cierto que existe g en las condiciones anteriores (algo que parece coherente), aún no se conoce a día de hoy. Esto último hace hincapié en el desconocimiento que sigue acompañando a los números de Carmichael, y desde luego parece oscurecer más cualquier aproximación a una de las respuestas buscadas. Sin embargo, aunque no se conoce cuál es el crecimiento asintótico exacto de la función C, es posible establecer algunos límites para el mismo. Dicho de otro modo, es posible acotar la función C. Una de las primeras cotas superiores fue aportada por el matemático austríaco Walter Knödel [Knö53], quien

en 1953 demostró que

$$C(x) < x \cdot e^{-c(\ln x \ \cdot \ \ln(\ln x))^{1/2}} \ , \tag{5.2}$$

para alguna constante positiva c. Algo más tarde, en 1956, Erdös [Erd56] consiguió probar la siguiente cota más fina

$$C(x) < x \cdot e^{-(1-\epsilon)\ln x \ \cdot \ \ln_3 x/\ln_2 x} \ , \tag{5.3}$$

válida para todo $\epsilon > 0$. A fin de simplificar la notación, escribimos $\ln_k x$ para referirnos al logaritmo natural iterado k veces (esta notación se ha empleado en (5.3)). La búsqueda de funciones que acoten C es un tema recurrente en el estudio analítico de los números de Carmichael (y es un tema habitual en la teoría analítica de números, reemplazando C por cualquier otra función aritmética). Como veremos, es suficiente con encontrar cotas lo suficientemente buenas para responder a las preguntas planteadas al comienzo de este capítulo.

Este sección tiene dos objetivos: dar una prueba con completo detalle de la cota para $C(x)$ presentada en (5.3) e introducir, sin demostración pero con rigor, algunos resultados importantes relacionados con los números de Carmichael.

5.1. Demostración de la cota de Erdös

Hasta este momento, todos los resultados han ido acompañandos de su demostración. Desgraciadamente, las pruebas de algunos de los resultados que se manejan en esta sección son verdaderamente complejas, e incluirlas en este trabajo supondría dedicar una buena parte del contenido a aspectos no relacionados con los números de Carmichael. Por ello, nos limitamos a enunciar algunos de los teoremas que utilizaremos. Éstos tienen por objetivo demostrar la validez de la cota introducida en (5.3). Aunque como hemos dicho la cota fue aportada por Erdös, seguiremos la reescritura de la prueba inicial que proporcionaron Pomerance, Selfridge y Wagstaff en [PSW80].

A fin de hacer la lectura más fácil, en este trabajo se incluyen todos los detalles de la demostración, incluyendo aquellos que los autores originales deciden no escribir por considerar elementales. Con el mismo objetivo de simplificar la lectura, comenzamos la demostración del Lema 5.1.4 mostrando el esquema que se sigue a lo largo de la prueba.

El primero de los resultados que nos ayudará a demostrar (5.3) está relacionado con la función

$$\begin{array}{rccc} \psi\colon & \mathbb{R}^2 & \longrightarrow & \mathbb{N} \\ & (x,y) & \longmapsto & |\{k \leq x : \text{ si } p \text{ es divisor primo de } k,\ p \leq y\}| \end{array}$$

Ésta ha sido exhaustivamente estudiada, y hoy en día se conoce todo un abanico de resultados sobre ella. En concreto, nos apoyaremos en el siguiente

Lema 5.1.1 (De Bruijn, [dB51]). *Para cada $\epsilon > 0$, existe $x_0(\epsilon)$ tal que, si $x > x_0(\epsilon)$, $\ln x \leq y \leq x$, $u = \ln x/\ln y$, entonces*

$$\psi(x,y) \leq x \cdot \exp(-(1-\epsilon)u\ln u) \ .$$

Haremos también uso del siguiente teorema, importante en teoría de números.

Teorema 5.1.2 (Rosser, [Ros39]). *Sea $(P_n)_n$ la sucesión de los números primos. Para todo natural n se cumple que $n\ln n < P_n < 2n\ln n$.*

El último de los resultados que se utilizarán es el siguiente.

Teorema 5.1.3 (Identidad de Abel [GHDH79])**.** *Para cada función aritmética a_n, definimos*

$$A(x) = \sum_{n \leq x} a(n) \ ,$$

donde $A(x) = 0$ si $x < 0$. Supongamos que $f(x)$ tiene una derivada continua en el intervalo $[x, y]$, con $0 < x < y$. Entonces

$$\sum_{x < n \leq y} a(n) f(n) = A(y) f(y) - A(x) f(x) - \int_x^y A(u) f'(u) du \ .$$

Recordamos que en el Capítulo 3 habíamos definido

$$L(n) = \text{mcm}(p - 1 : p \text{ es divisor primo de } n) \ .$$

Definimos el conjunto

$$B_t(y) := \{k \leq y : L(k) = t\} \ , \tag{5.4}$$

como las "soluciones" al problema de encontrar enteros positivos k, menores o iguales a y, que cumplen $L(k) = t$ para un t dado. Dicho de otro modo, estamos interesados en acotar el cardinal de los conjuntos $L^{-1}(t) \cap \{1, 2, \ldots, y\}$.

Lema 5.1.4. *Para cada $\epsilon > 0$, existe $y_0(\epsilon)$ de modo que*

$$|B_t(y)| \leq y \cdot \exp(-(1 - \epsilon) \ln y \cdot \ln_3 y / \ln_2 y) \ ,$$

para todo $y \geq y_0(\epsilon)$ y todo t natural.

Demostración. Para esta demostración, seguimos los siguientes pasos (aunque se repite la notación que surge de forma natural a lo largo de la prueba, la incluimos aquí para que al lector le resulte más sencillo situarse una vez comenzada la lectura):

1. En primer lugar, observamos que es suficiente con demostrar la validez de la cota para todo $\epsilon > 0$ por debajo que una cierta cantidad $\xi > \epsilon > 0$. En esta prueba, tomamos $\xi = 1/21$ (tomaremos $1/3 > \delta$ y concluiremos que el resultado es cierto para $\epsilon = \delta/7$).

2. Comprobamos que el resultado se cumple al tomar $t = 1$.

3. Definimos los conjuntos U, U_1, U_2 y $\alpha = \ln_3 y / \ln_2 y$.

4. Demostramos que, si $t \geq 2$ y $1/3 > \delta > 0$, si r_i es el i-ésimo elemento de U_2 cuando sus elementos se ordenan crecientemente, entonces $r_i > P_i^{1+(1-3\delta)\alpha}$ para y suficientemente grande. A su vez, dividimos esta tarea en 3 casos:

   - $i = 1$
   - $1 < i \leq \exp((\ln_2 y)^2 / 6 \ln_3 y)$
   - $\exp((\ln_2 y)^2 / 6 \ln_3 y) < i$ (acarrea una buena parte de la prueba, pags. ón 1-37)

5. Definimos los conjuntos K_q y K_r. De igual manera, si $A \subset \mathbb{N}$ y $\lambda \in \mathbb{R}$, definimos $N(A, \lambda) = |\{a \in A : a \leq \lambda\}|$.

6. Haciendo uso de la desigualdad del punto 4, demostramos que $N(K_r, \omega) \leq \omega^{1-(1-4\delta)\alpha}$.

7. Aplicando el Lema 5.1.1, demostramos que $N(K_q, \omega) \leq \omega^{1-(1-2\delta)\alpha}$.

8. Descomponemos $|B_t(y)|$ como sumas extendidas a los conjuntos K_r y K_q. Reducimos las sumas a dos sumatorios independientes sobre el conjunto K_q y tratamos de acotarlas. En concreto, para el segundo sumatorio aplicamos el Teorema 5.1.3.

9. Comprobamos que, tomando $\delta = \epsilon/6$, se demuestra la cota.

Comenzamos observando que basta con demostrar que el resultado es cierto para todo ϵ menor que un cierto número positivo. En efecto, asumamos que el resultado es cierto para todo $\lambda \leq \xi$ y tomemos $\epsilon > \xi$. No es difícil comprobar que

$$y \cdot \exp(-(1-\epsilon)\ln y \cdot \ln_3 y/\ln_2 y) = y \cdot \exp(-\ln y \cdot \ln_3 y/\ln_2 y) \cdot \exp(\epsilon \ln y \cdot \ln_3 y/\ln_2 y) > \\ > y \cdot \exp(-\ln y \cdot \ln_3 y/\ln_2 y) \cdot \exp(\xi \ln y \cdot \ln_3 y/\ln_2 y) \geq |B_t(y)| \ .$$

El caso $t = 1$ es claro ya que $|B_t(y)| \leq \log_2 y$ (solamente en este caso $\log_2 y$ denota al logaritmo en base 2, y este es el único punto en que nos referimos a un logaritmo en base diferente a e). En efecto, $L(k) = 1$ solamente si, $p - 1 = 1$ para todo factor primo p de k. En consecuencia, $p = 2$ es el único factor primo permitido, y k debe ser una potencia de 2. Además, para y suficientemente grande

$$\log_2(y) \leq y \cdot \exp(-(1-\epsilon)\ln y \cdot \ln_3 y/\ln_2 y) = y^{\epsilon} \ ,$$

mayor que cualquier logaritmo.

Asumimos que $t \geq 2$. Definimos los siguientes conjuntos

$$U = \{p : (p-1)|t \ , \ p \text{ es primo}\} \ ,$$
$$U_1 = \{q \in U : q \leq \exp((\ln_2 y)^2/\ln_3 y) \ \} \ ,$$
$$U_2 = \{r \in U : r > \exp((\ln_2 y)^2/\ln_3 y) \ \} \ .$$

Resulta inmediato comprobar que los conjuntos U_1, U_2 forman una partición del conjunto U. Denotaremos además por r_i al i-ésimo elemento del conjunto U_2, con éstos ordenados crecientemente.

Sea $1/3 > \delta > 0$. Escribiremos $\alpha = \ln_3 y/\ln_2 y$. A continuación, veamos que existe un número real $y_1(\delta)$ satisfaciendo que, para cada i tal que r_i es un elemento de U_2, si $y \geq y_1(\delta)$ entonces

$$r_i > P_i^{1+(1-3\delta)\alpha} \ , \tag{5.5}$$

donde P_i denota al i-ésimo número primo.

Dado que α es una función (que está definida para todo real mayor que e) decreciente a partir de una cierta cantidad, escogiendo $y_1(\delta)$ suficientemente grande se verifica que $\alpha < 1$. En consecuencia, puede garantizarse que $r_1 > 4$, cumpliéndose además que $r_1 > 2^2 = P_1^2 > P_1^{1+(1-3\delta)\alpha}$.

Supongamos ahora que $1 < i \leq \exp((\ln_2 y)^2/6\ln_3 y)$. Se cumple

$$r_i > i^6 > (2i\ln i)^2 > P_i^2 > P_i^{1+(1-3\delta)\alpha} \ .$$

La primera de las desigualdades está justificada por el hecho de que $i^6 \leq \exp((\ln_2 y)^2/\ln_3 y) < r_i$. Para la segunda, dado que $i \geq 2$ y que $\ln i < i$, debe cumplirse que $(2i \ln i)^2 < i^6$. La validez de la tercera está garantizada por el Teorema 5.1.2. La última desigualdad vuelve a ser inmediata, pues al igual que antes, se tiene que $2 > 1 + (1 - 3\delta)\alpha$.

Queda por estudiar el caso $i > \exp((\ln_2 y)^2/6 \ln_3 y)$. A fin de comprobar que la cota (5.5) sigue siendo válida, es últil observar que la función

$$v(x) = \delta\alpha \ln x - 2 \ln_2 x \ , \tag{5.6}$$

es creciente para todo $x > \max\{(\ln y)^{2/(\delta \ln_3 y)}, 1\}$ (escribimos está expresión para garantizar que $\ln_2 x$ está definido). En efecto,

$$v'(x) = \frac{\delta\alpha}{x} - \frac{2}{x \ln x} = \frac{1}{x}\left(\delta\alpha - \frac{2}{\ln x}\right) \ ,$$

de modo que $v'(x) > 0$ siempre que $\ln x > 2/(\delta\alpha) = (2/\delta)(\ln_2 y/\ln_3 y)$, o alternativamente, siempre que $x > \max\{(\ln y)^{2/(\delta \ln_3 y)}, 1\}$. Por otra parte, si $y \geq y_2(\delta)$ para $y_2(\delta)$ suficientemente grande, se cumple que

$$i > (\ln y)^{3/\delta} > (\ln y)^{2/(\delta \ln_3 y)} \ .$$

Para verlo, reescribamos $\exp((\ln_2 y)^2/6 \ln_3 y) = (\ln y)^{\ln_2 y/(6 \ln_3 y)}$. Observemos ahora que $\alpha^{-1} = \ln_2 x/\ln_3 x$ no está acotado, y que por tanto

$$\ln_2 y/(6 \ln_3 y) > 3/\delta$$

si $y \geq y_2(\delta)$. En consecuencia, $i > \exp((\ln_2 y)^2/6 \ln_3 y) = (\ln y)^{\ln_2 y/(6 \ln_3 y)} > (\ln y)^{3/\delta}$. La segunda desigualdad es clara teniendo en cuenta que $\ln_3 y > 1$. Dado que i está dentro del intervalo en que v es creciente, se sigue que

$$\begin{aligned} \delta\alpha \ln i - 2 \ln_2 i > \delta\alpha(3/\delta) \ln_2 y - 2 \ln(3/\delta) - 2 \ln_3 y = \\ = 3(\ln_3 y/\ln_2 y) \ln_2 y - 2 \ln(3/\delta) - 2 \ln_3 y = \ln_3 y - 2 \ln(3/\delta) > \ln 4 \ . \end{aligned}$$

La desigualdad anterior puede reescribirse como

$$\delta\alpha \ln i > 2 \ln_2 i + \ln 4 = \ln((2 \ln i)^2) \ ,$$

o equivalentemente

$$i^{\delta\alpha} > (2 \ln i)^2 \ . \tag{5.7}$$

Consideramos ahora la lista completa s_1, s_2, ..., s_m de los divisores de t. Por la definición de U, para cada $r \in U_2$ se tiene que $(r-1)|t$. En consecuencia, todos los factores primos de $r - 1$ están en la lista s_1, s_2, ..., s_m. Teniendo esto en cuenta, así como que existen exactamente i elementos $r \in U_2$ tales que $r \leq r_i$, las siguiente desigualdad se deduce de forma directa

$$i \leq \psi(r_i, P_m) \ ,$$

donde ψ es la función del Lema 5.1.1 y, como venimos escribiendo en este capítulo, P_m es el m-ésimo número primo. Por otra parte, existe una constante $c > 0$ tal que $P_m < c \ln t$. En efecto, cualquier número con más de m factores primos distintos es mayor que $\prod_{l=1}^{m} P_l$. En consecuencia, tenemos que

$$\frac{\ln t}{P_m} \geq \frac{\ln\left(\prod_{l=1}^{m} P_l\right)}{P_m} > \frac{\ln(m!)}{P_m} \ .$$

Recordando la aproximación de Stirling $\ln n! \sim n\ln n - n$, así como que por el teorema del número primo se cumple $P_n \sim n\ln n$, puede escribirse

$$\frac{\ln(m!)}{P_m} \sim \frac{m\ln m - m}{m\ln m} = 1 - \frac{1}{\ln m} \longrightarrow 1 \ ,$$

de modo que existe $c \geq 1$ tal que $P_m < c\ln t$. Siguiendo con la prueba, se cumple que

$$i \leq \psi(r_i, P_m) \leq \psi(r_i, c\ln t) \leq \psi(r_i, c\ln y) \ .$$

Definiendo $z = y^c$, tenemos

$$\psi(r_i, c\ln y) = \psi(r_i, \ln z)$$

Ahora bien, dado que $r_i \leq y \leq z$ y recordando que por definición $r_i > \exp((\ln_2 y)^2/\ln_3 y)$, se cumple que $\ln r_i \leq \ln z = \ln y^c \leq r_i$ siempre que $z \geq z_3(\delta)$. Por el Lema (5.1.1),

$$\psi(r_i, \ln z) \leq r_i \exp(-(1-\delta)\tilde{u_i}\ln\tilde{u_i}) \ ,$$

donde $\tilde{u_i} = \ln r_i/(\ln_2 z)$. Sin embargo, escogiendo $y_3(\delta) = (z_3(\delta))^{1/c}$, podemos asegurar que para $y \geq y_3(\delta)$

$$\psi(r_i, c\ln y) \leq r_i \exp(-(1-\delta)u_i\ln u_i) \ ,$$

donde $u_i = \ln r_i/\ln_2 y$. Haciendo uso otra vez de que $r_i > \exp((\ln_2 y)^2/\ln_3 y)$ se deriva fácilmente que $u_i = \ln r_i/\ln_2 y > \ln_2 y/\ln_3 y$. A continuación, demostramos la siguiente desigualdad

$$-(1-\delta)u_i\ln u_i < -(1-2\delta)u_i\ln_3 y \ . \tag{5.8}$$

En efecto, partiendo de

$$(\ln_2 y)^{1+(1-\delta)/(1-2\delta)} \geq \ln_3 y \ ,$$

se sigue

$$\frac{\ln_2 y}{\ln_3 y} > (\ln_2 y)^{(1-2\delta)/(1-\delta)} \ .$$

Como $r_i > \exp((\ln_2 y)^2/\ln_3 y)$,

$$\begin{aligned} u_i = \frac{\ln r_i}{\ln_2 y} &> (\ln_2 y)^{(1-2\delta)/(1-\delta)} \ , \\ \ln u_i &> \frac{(1-2\delta)}{(1-\delta)}\ln_3 y \ , \\ (1-\delta)\ln u_i &> (1-2\delta)\ln_3 y \ , \end{aligned}$$

lo que prueba (5.8). En consecuencia, se deriva que

$$i \leq r_i\exp(-(1-\delta)u_i\ln u_i) < r_i\exp(-(1-2\delta)u_i\ln_3 y) = r_i\exp(-(1-2\delta)\alpha\ln r_i) = r_i^{1-(1-2\delta)\alpha} \ .$$

Teniendo en cuenta que $i > 1$, se verifica

$$r_i > i^{(1-(1-2\delta)\alpha)^{-1}} > i^{1+(1-2\delta)\alpha} \ .$$

Finalmente, haciendo uso de (5.7) y el Teorema 5.1.2, para todo y mayor o igual que $y_4(\delta) = \max\{y_1(\delta), y_2(\delta), y_3(\delta)\}$, se cumple que

$$r_i > i^{1+(1-2\delta)\alpha} = i^{1+(1-3\delta)\alpha+\delta\alpha} > i^{1+(1-3\delta)\alpha}\cdot(2\ln i)^2 > (2i\ln i)^{1+(1-3\delta)\alpha} > P_i^{1+(1-3\delta)\alpha} \ , \tag{5.9}$$

donde se ha utilizado que $1 + (1 - 3\delta)\alpha < 2$. Hemos demostrado la desigualdad (5.5).

Definimos dos conjuntos adicionales,

$$K_r = \{R : \forall\ p \text{ factor primo de } R,\ p \in U_2\}\ ,$$
$$K_q = \{Q : \forall\ p \text{ factor primo de } Q,\ p \in U_1\}\ .$$

Adicionalmente, definimos la función N que cuenta los elementos menores o iguales que $\omega \geq 1$ dentro de los conjuntos anteriores

$$N(K_r, \omega) := |\{R \in K_r : R \leq \omega\}|\ ,$$
$$N(K_q, \omega) := |\{Q \in K_q : Q \leq \omega\}|\ .$$

Llamando a al mayor índice i tal que $r_i \in U_2$, para $y \geq y_4(\delta)$ se cumple que $r_i^{(1+(1-3\delta)\alpha)^{-1}} > P_i$ en virtud de la desigualdad (5.5), y podemos escribir

$$N(K_r, w) \leq N(\{P_1, P_2, \ldots, P_a\}, \omega^{(1+(1-3\delta)\alpha)^{-1}}) \leq \omega^{(1+(1-3\delta)\alpha)^{-1}}\ .$$

Observemos ahora que se la desigualdad $(1 + (1 - 3\delta)\alpha)^{-1} \leq 1 - (1 - 4\delta)\alpha$. Partiendo de $(1 - 3\delta)^2\alpha \leq \delta + \delta(1 - 3\delta)\alpha$, que es claramente cierta porque $(1 - 3\delta) < 1$, se deriva que

$$(1 - 3\delta)^2\alpha^2 \leq \delta\alpha + \delta(1 - 3\delta)\alpha^2\ ,$$
$$1 \leq 1 - (1 - 3\delta)^2\alpha^2 + \delta\alpha + \delta(1 - 3\delta)\alpha^2 = 1 \leq (1 + (1 - 3\delta)\alpha)(1 - (1 - 4\delta)\alpha)\ ,$$

de donde se deduce la desigualdad buscada. Por lo tanto

$$N(K_r, w) \leq w^{1-(1-4\delta)\alpha}\ . \tag{5.10}$$

Se tiene además, por la definición de U_1,

$$N(K_q, w) \leq \psi(w, \exp((\ln_2 y)^2/\ln_3 y))\ .$$

Si adicionalmente $\exp((\ln_2 y)^2/\ln_3 y) \geq w \geq y^\delta$, para $y \geq y_5(\delta)$ suficientemente grande se cumple

$$\ln w > \delta \ln y > (\ln_2 y)^2/\ln_3 y\ ,$$

y estamos en condiciones de aplicar el Lema 5.1.1. Entonces,

$$N(K_q, w) \leq \psi(w, \exp((\ln_2 y)^2/\ln_3 y)) \leq w \exp(-(1 - \delta)u \ln u)\ ,$$

con $u = \ln w \cdot \ln_3 y/(\ln_2 y)^2$. Además, si $y \geq y_6(\delta)$ es suficientemente grande se cumple $\ln u/\ln_2 y < 1$ y podemos escribir

$$N(K_q, w) \leq w \exp(-(1 - \delta)\alpha \ln w) \leq w \exp(-(1 - 2\delta)\alpha \ln w)\ . \tag{5.11}$$

Tomando ahora $y_7(\delta) = \max\{y_4(\delta), y_5(\delta), y_6(\delta)\}$, por (5.11) y (5.10) tenemos que para $y \geq y_7(\delta)$

$$|B_k(y)| = |\{k \le y : L(k) = t\}| \le |\{k \le y : k = QR,\ Q \in K_q, R \in K_r\}| = \sum_{\substack{Q\in K_q \\ Q\le y}} \sum_{\substack{R\in K_r \\ R\le (y/Q)}} 1 =$$

$$= \sum_{\substack{Q\in K_q \\ Q\le y}} N(K_r,(y/Q)) \le \sum_{\substack{Q\in K_q \\ Q\le y}} \left(\frac{y}{Q}\right)^{1-(1-4\delta)\alpha} = y^{1-(1-4\delta)\alpha} \sum_{\substack{Q\in K_q \\ Q\le y}} \left(\frac{1}{Q}\right)^{1-(1-4\delta)\alpha} =$$

$$= y^{1-(1-4\delta)\alpha} \left(\sum_{\substack{Q\in K_q \\ Q\le y^\delta}} \left(\frac{1}{Q}\right)^{1-(1-4\delta)\alpha} + \sum_{\substack{Q\in K_q \\ y^\delta < Q\le y}} \left(\frac{1}{Q}\right)^{1-(1-4\delta)\alpha} \right) . \tag{5.12}$$

Ahora, tratamos de acotar superiormente cada uno de los sumatiorios. El primero de ellos puede extenderse a todos los números naturales menores o iguales que y^δ, i.e. puede suprimirse la restricción $Q \in K_q$, obteniendo

$$\sum_{\substack{Q\in K_q \\ Q\le y^\delta}} \left(\frac{1}{Q}\right)^{1-(1-4\delta)\alpha} \le \sum_{n\le y^\delta} \left(\frac{1}{n}\right)^{1-(1-4\delta)\alpha} = \sum_{n\le y^\delta} n^{(1-4\delta)\alpha-1} .$$

Ahora bien, como $(1-4\delta)\alpha - 1 < \alpha$, puede escribirse

$$\sum_{n\le y^\delta} n^{(1-4\delta)\alpha-1} \le \sum_{n\le y^\delta} n^\alpha \le \left(\sum_{n\le y^\delta} n\right)^\alpha \le y^{2\delta\alpha} .$$

A continuación tratamos de acotar el segundo sumatorio, haciendo uso de la Identidad de Abel (Teorema 5.1.3). Manteniendo la notación del teorema, tomamos $f(x) = x^{(1-4\delta)\alpha-1}$ (que tiene una derivada continua para todo $x > 0$) y $a(n) = \chi_{K_q}(n)$ la función característica del conjunto K_q (1 si $n \in K_q$, 0 si $n \notin K_q$). Con esta elección, se tiene

$$A(x) = |B_{K_q}(x)| = N(K_q, x) .$$

En virtud del teorema, se sigue que

$$\sum_{\substack{Q\in K_q \\ y^\delta < Q\le y}} \left(\frac{1}{Q}\right)^{1-(1-4\delta)\alpha} = \sum_{y^\delta < n\le y} n^{(1-4\delta)\alpha-1}\chi_{K_q}(n) =$$

$$= y^{(1-4\delta)\alpha-1}\cdot N(K_q,y) - y^{(1-4\delta)\alpha\delta-\delta}\cdot N(K_q,y^\delta) + \frac{1}{1-(1-4\delta)\alpha}\int_{y^\delta}^{y} \frac{N(K_q,u)}{u^{2-(1-4\delta)\alpha}}du <$$

$$< y^{(1-4\delta)\alpha-1}\cdot N(K_q,y) + 2\int_{y^\delta}^{y} \frac{N(K_q,u)}{u^{2-(1-4\delta)\alpha}}du , \tag{5.13}$$

donde en la última desigualdad se ha eliminado el sumando negativo y se ha hecho uso de que $1-(1-4\delta)\alpha > 1/2$ para y suficientemente grande.

Recordando la Eq.(5.11), podemos escribir

$$y^{(1-4\delta)\alpha-1}\cdot N(K_q,y) + 2\int_{y^\delta}^{y} \frac{N(K_q,u)}{u^{2-(1-4\delta)\alpha}}du < \frac{y^{1-(1-2\delta)\alpha}}{y^{1-(1-4\delta)\alpha}} + 2\int_{y^\delta}^{y} \frac{u^{1-(1-2\delta)\alpha}}{u^{2-(1-4\delta)\alpha}}du <$$

$$< y^{-2\alpha\delta} + 2\int_{y^\delta}^{y} u^{-1-2\alpha\delta} < y^{-2\alpha\delta} + \frac{-1}{\alpha\delta}\left(y^{-2\alpha\delta} - y^{-2\alpha\delta^2}\right) < 2y^{-2\alpha\delta} . \tag{5.14}$$

Con todo lo anterior, concluímos que

$$\begin{aligned} |B_t(y)| &\leq y^{1-(1-4\delta)\alpha}(y^{2\alpha\delta} + 2y^{-2\alpha\delta}) \leq \\ &\leq y^{1-(1-6\delta)\alpha} + 2y^{1-(1-2\delta)\alpha} < y^{1-(1-7\delta)\alpha} \end{aligned} \tag{5.15}$$

Escogiendo $\delta = \epsilon/7$, se obtiene el resultado. □

Una vez demostrado el Lema 5.1.4 anterior, procedemos a demostrar la cota de la Eq.(5.3).

Teorema 5.1.5. *Sea $\epsilon > 0$. Existe $x_0(\epsilon)$ tal que, si $x > x_0(\epsilon)$, entonces*

$$C(x) \leq x \exp\left(-(1-\epsilon)\ln x \cdot \ln_3 x / \ln_2 x\right) .$$

Demostración. Podemos asumir que $x \geq 561$, el primer número de Carmichael. Por el mismo argumento que en el comienzo de la demostración del lema anterior, podemos limitarnos a probar el resultado para los ϵ menores que un cierto número positivo.

Sea $1/3 > \delta > 0$. Dividimos los números de Carmichael $n \leq x$ en tres clases:

1. $n \leq x^{1-\delta}$
2. $x^{1-\delta} < n \leq x$ y n tiene un factor primo $p \geq x^{\delta}$
3. $x^{1-\delta} < n \leq x$ y todo factor primo de n es menor que x^{δ}.

Encontraremos una cota superior para la cantidad de números de Carmichael en cada clase, que denotamos por N_1, N_2 y N_3. Claramente, se tiene que $N_1 \leq x^{1-\delta}$.

Continuamos con la segunda clase. Sea n perteneciente a ésta y p un factor primo satisfaciendo que $p \geq x^{\delta}$. Es claro que, por ser n de Carmichael, deben satisfacerse las siguientes dos congruencias (criterio de Korselt),

$$n \equiv 0 \pmod{p} \quad , \quad n \equiv 1 \pmod{p-1} .$$

Ahora bien, dado que $(p, p-1) = 1$, el teorema chino de los restos garantiza que existe un único representante en $\mathbb{Z}/p(p-1)\mathbb{Z}$ satisfaciendo las anteriores congruencias. Esto significa que, entre dos múltiplos consecutivos de $p(p-1)$, solo podrá haber un número de Carmichael que tenga a p por factor. Esta observación permite escribir

$$N_2 \leq x \sum_{p \geq x^{\delta}}^{x} \frac{1}{p(p-1)} \leq x \sum_{n \geq x^{\delta}}^{x} \frac{1}{n(n-1)} = x \sum_{n \geq x^{\delta}}^{x} \left(\frac{1}{n-1} - \frac{1}{n}\right) = x\left(\frac{1}{x^{\delta}-1} - \frac{1}{x}\right) ,$$

donde la última igualdad puede escribirse debido a que los términos del sumatorio se anulan entre sí. Se sigue que

$$N_2 \leq x\left(\frac{1}{x^{\delta}-1} - \frac{1}{x}\right) = x\left(\frac{x - x^{\delta} + 1}{x(x^{\delta}-1)}\right) < x\left(\frac{x+1}{x(x^{\delta}-1)}\right) .$$

Para x suficientemente grande, se verifica la desigualdad

$$\frac{1}{x} + \frac{2}{x^{\delta}} < 1 .$$

Se sigue que

$$1 + \frac{1}{x} < 2\left(1 - \frac{1}{x^\delta}\right) = 2\left(\frac{x^\delta - 1}{x^\delta}\right) \ ,$$

o equivalentemente

$$\frac{x+1}{x(x^\delta - 1)} < \frac{2}{x^\delta} \ .$$

En consecuencia, se tiene que $N_2 < 2x^{1-\delta}$.

Solo queda acotar N_3. Veamos que si n pertenece a la tercera clase, entonces n tiene un divisor $x^{1-2\delta} < k \leq x^{1-\delta}$. Sabemos que $n = p_1 p_2 \dots p_s$ es libre de cuadrados (criterio de Korselt), y $p_i < x^\delta$ para todo $1 \leq i \leq s$. Definimos el conjunto

$$D = \{d : d \text{ es divisor de } n \text{ y } d > x^{1-2\delta}\} \ .$$

D es obviamente finito y no vacío, ya que dado un divisor primo p de n, se tiene

$$d = \frac{n}{p} > \frac{n}{x^\delta} > \frac{x^{1-\delta}}{x^\delta} = x^{1-2\delta} \ ,$$

y $d \in D$ (obviamente, también se tiene que $n \in D$). Consideramos $k = \min D$. Por ser k un divisor de n, debe ser $k = p_{i_1} p_{i_2} \dots p_{i_r}$, con $\{i_1, i_2, \dots, i_r\} \subset \{1, 2, \dots, s\}$, $r \geq 1$. Por la definición de k, se sigue que $k/p_{i_1} \notin D$, y por tanto $k/p_{i_1} \leq x^{1-2\delta}$. En consecuencia, $k = (k/p_{i_1})p_{i_1} \leq x^{1-2\delta} x^\delta = x^{1-\delta}$ y n tiene un divisor en las condiciones buscadas.

Veamos ahora la siguiente desigualdad,

$$|\{n \leq x : n \text{ es de Carmichael, } k|n\}| \leq 1 + \frac{x}{kL(k)} \ . \tag{5.16}$$

Comenzamos comprobando que $(k, L(k)) = 1$. En efecto, por ser n de Carmichael,

$$n \equiv 0 \pmod{k} \quad , \quad n \equiv 1 \pmod{L(k)} \ .$$

Escribiendo $g = (k, L(k))$, las anteriores congruencias implican

$$n \equiv 0 \pmod{g} \quad , \quad n \equiv 1 \pmod{g} \ ,$$

de modo que $0 \equiv 1 \pmod{g}$. Por tanto debe ser $g = 1$. Razonando de igual manera que en la cota de N_1, es posible aplicar el teorema chino de los restos para verificar que entre dos múltiplos consecutivos de $kL(k)$, solo podrá haber un número de Carmichael que tenga a k por divisor. En consecuencia, se sigue la desigualdad (5.16). Podemos acotar N_3 como

$$N_3 \leq \sum_{x^{1-2\delta} < k \leq x^{1-\delta}} \left(1 + \frac{x}{kL(k)}\right) \leq x^{1-\delta} + \sum_{x^{1-2\delta} < k \leq x^{1-\delta}} \frac{x}{kL(k)}$$

Podemos reescribir el sumatorio de la última igualdad como

$$N_3 \leq x^{1-\delta} + \sum_{d \leq x} \frac{x}{d} \sum_{\substack{x^{1-2\delta} < k \leq x^{1-\delta} \\ L(k) = d}} \frac{1}{k} \ .$$

Nos concentramos ahora en el sumatorio interno. Teniendo en cuenta que la función $1/x$ tiene una derivada continua para todo $x > 0$, podemos aplicar la identidad de Abel (Teorema 5.1.3). Manteniendo la notación de su enunciado, escogemos $f = 1/x$ y $a(n) = \chi_{B_d(n)}$

la función característica del conjunto $B_d(n)$ (1 si $n \in B_d(n)$, 0 si $n \notin B_d(n)$). Con esta elección de $a(n)$, se sigue que $A(x) = |B_d(x)|$. El teorema conduce a que

$$\begin{aligned} \sum_{\substack{x^{1-2\delta}<k\leq x^{1-\delta} \\ L(k)=d}} \frac{1}{k} = \sum_{x^{1-2\delta}<k\leq x^{1-\delta}} \left(\chi_{B_d(k)}\frac{1}{k}\right) = \\ = \frac{1}{x^{1-\delta}}|B_d(x^{1-\delta})| - \frac{1}{x^{1-2\delta}}|B_d(x^{1-2\delta})| + \int_{x^{1-2\delta}}^{x^{1-\delta}} \frac{1}{u^2}|B_d(u)|du \ . \end{aligned} \tag{5.17}$$

Es evidente (sumandos positivos) que

$$\frac{1}{x^{1-\delta}}|B_d(x^{1-\delta})| - \frac{1}{x^{1-2\delta}}|B_d(x^{1-2\delta})| \leq \frac{1}{x^{1-\delta}}|B_d(x^{1-\delta})| \ . \tag{5.18}$$

Para x suficientemente grande, el Lema 5.1.4 permite afirmar que

$$\begin{aligned} \frac{1}{x^{1-\delta}}|B_d(x^{1-\delta})| \leq \frac{1}{x^{1-\delta}} \cdot x^{1-\delta} \exp\left(-(1-\delta)(1-\delta)\ln x \ln_3 x^{1-\delta}/\ln_2 x^{1-\delta}\right) = \\ = \exp\left(-(1-2\delta+\delta^2)\ln x \ln_3 x^{1-\delta}/\ln_2 x^{1-\delta}\right) < \exp\left(-(1-2\delta)\ln x \ln_3 x^{1-\delta}/\ln_2 x^{1-\delta}\right) \ . \end{aligned} \tag{5.19}$$

Tratamos de acotar la integral de la Ec.(5.17). Haciendo uso de nuevo del Lema 5.1.4, para x suficientemente grande se sigue que

$$|B_d(u)| \leq u \exp\left(-(1-\delta)\ln u \ln_3 u/\ln_2 u\right) \ . \tag{5.20}$$

Sustituyendo en el integrando

$$\begin{aligned} \frac{1}{u^2}|B_d(u)| \leq \frac{1}{u}\exp\left(-(1-\delta)\ln u \ln_3 u/\ln_2 u\right) \leq \\ \leq \frac{1}{u}\exp\left(-(1-\delta)(1-2\delta)\ln x \ln_3 x^{1-2\delta}/\ln_2 x^{1-2\delta}\right) < \\ < \frac{1}{u}\exp\left(-(1-3\delta)\ln x \ln_3 x^{1-2\delta}/\ln_2 x^{1-2\delta}\right) \ . \end{aligned} \tag{5.21}$$

Por tanto

$$\begin{aligned} \int_{x^{1-2\delta}}^{x^{1-\delta}} \frac{1}{u^2}|B_d(u)|du < \exp\left(-(1-3\delta)\ln x \ln_3 x^{1-2\delta}/\ln_2 x^{1-2\delta}\right) \int_{x^{1-2\delta}}^{x^{1-\delta}} \frac{du}{u} = \\ = \exp\left(-(1-3\delta)\ln x \ln_3 x^{1-2\delta}/\ln_2 x^{1-2\delta}\right)\Big[\ln u\Big]_{x^{1-2\delta}}^{x^{1-\delta}} = \\ = \delta \ln x \cdot \exp\left(-(1-3\delta)\ln x \ln_3 x^{1-2\delta}/\ln_2 x^{1-2\delta}\right) \ . \end{aligned}$$

Realizando la observación de que $\ln_3 y/\ln_2 y$ es una función decreciente para y suficientemente grande (tiene límite 0 en el infinito), podemos escribir

$$\frac{\ln_3 x^{1-2\delta}}{\ln_2 x^{1-2\delta}} > \frac{\ln_3 x^{1-\delta}}{\ln_2 x^{1-\delta}} > \frac{\ln_3 x}{\ln_2 x} \ .$$

Consecuentemente,

$$\sum_{\substack{x^{1-2\delta}<k\leq x^{1-\delta} \\ L(k)=d}} \frac{1}{k} < \exp\left(-(1-2\delta)\ln x \ln_3 x/\ln_2 x\right) + \delta \ln x \cdot \exp\left(-(1-3\delta)\ln x \ln_3 x/\ln_2 x\right) <$$

$$< (1+\delta\ln x)\cdot \exp\left(-(1-3\delta)\ln x \ln_3 x/\ln_2 x\right) = \ln(e\cdot x^{\delta})\cdot \exp\left(-(1-3\delta)\ln x \ln_3 x/\ln_2 x\right) \ ,$$

obteniéndose

$$\sum_{\substack{x^{1-2\delta}<k\leq x^{1-\delta}\\ L(k)=d}} \frac{1}{k} < \ln x \cdot \exp\left(-(1-3\delta)\ln x \ln_3 x/\ln_2 x\right) . \tag{5.22}$$

Por tanto, puede acotarse N_3 como

$$N_3 < x^{1-\delta} + x\ln x \cdot \exp\left(-(1-3\delta)\ln x \ln_3 x/\ln_2 x\right)\sum_{d\leq x}\frac{1}{d} . \tag{5.23}$$

Notemos que $\sum_{d\leq x}\frac{1}{d} \leq \ln x + \gamma$. Además, como $\lim(\ln x \ln_3 x)/(\ln_2 x)^3 = \infty$, para x suficientemente grande se tiene

$$\ln^2 x = \exp\left(2\ln_2 x\right) < \exp\left(\delta \ln x \ln_3 x/\ln_2 x\right) .$$

Con las anteriores desigualdades, podemos escribir

$$N_3 < x^{1-\delta} + x\exp\left(-(1-5\delta)\ln x \ln_2 x/\ln_3 x\right) .$$

Finalmente, la función $C(x)$ puede acotarse como

$$\begin{aligned} C(x) = N_1 + N_2 + N_3 < x^{1-\delta} + 2x^{1-\delta} + x^{1-\delta} + x\cdot\exp\left(-(1-5\delta)\ln x\ln_3 x/\ln_2 x\right) = \\ = 4x^{1-\delta} + x\cdot\exp\left(-(1-5\delta)\ln x\ln_3 x/\ln_2 x\right) = x\cdot\left(4x^{-\delta} + \exp\left(-(1-5\delta)\ln x\ln_3 x/\ln_2 x\right)\right) < \\ < x\cdot\exp\left(-(1-6\delta)\ln x\ln_3 x/\ln_2 x\right) . \end{aligned}$$

Y tomando $\epsilon = 6\delta$, tenemos el resultado. □

5.2. Existencia de infinitos números de Carmichael

Volviendo a las preguntas con las que introdujimos este capítulo, hay una que tiene una relevancia especial: ¿existen infinitos números de Carmichael? Aunque en la sección anterior hemos demostrado la validez de una cota superior, desgraciadamente esto no es suficiente a la hora de afirmar o desmentir la cuestión anterior. Otra cosa sería que hubieramos demostrado una cota inferior. En efecto, bastaría con que la función que acota inferiormente no estuviera acotada para poder garantizar que, por ende, tampoco lo está C. Durante años la búsqueda de esta cota inferior fue uno de los temas de investigación centrales en relación a los números de Carmichael. En el mismo artículo en que Erdös publicó la cota que sí hemos probado, desarrolló un argumento heurístico en que apuntaba a una posible cota inferior. Sin embargo, no fue hasta 1994 cuando W. R. Alford, Andrew Granville and Carl Pomerance obtuvieron por primera vez una cota de este tipo, en parte inspirados por las ideas de Erdös.

A fin de contextualizar los resultados de [AGP94], comenzamos discutiendo la precisión de la cota asintótica en el teorema del número primo para progresiones aritméticas. El enunciado más habitual de este teorema es el siguiente.

Teorema 5.2.1 ([Dab89])**.** *Sean $0 < a < d$ con $(a,d) = 1$. Denotamos por $\pi(x;d,a)$ a la cantidad de números primos no mayores que x pertenecientes a la progresión aritmética a* (mód d)*. Entonces*

$$\pi(x;d,a) \to \pi(x)/\varphi(d), \text{ cuando } x\to\infty .$$

En otras palabras,

$$\pi(x;d,a) = (1+o(1))\frac{1}{\varphi(d)}\frac{x}{\ln x}$$

donde $o(1) \to 0$ *cuando* $x \to \infty$.

Al igual que en el teorema del número primo estándar, el interés actual en este resultado reside en la "rapidez" con la que $\pi(x;d,a)$ se aproxima a $\pi(x)/\varphi(d)$, i.e. en estimar de forma precisa el valor de $o(1)$. Para ahondar en esta cuestión (y como una herramienta necesaria en la demostración tanto del Teorema 5.2.1 como del teorema del número primo), recordamos la siguiente conocida función aritmética.

Definición 5.2.2 (Función de Mangoldt)**.** La función $\Lambda : \mathbb{N} \to \mathbb{R}$ dada por

$$\Lambda(n) = \begin{cases} \ln p & \text{si } n = p^\alpha \\ 0 & \text{en otro caso} \end{cases} \tag{5.24}$$

se conoce como función de Mangoldt.

Es sencillo realizar la siguiente observación

$$\ln n = \sum_{u|n} \Lambda(n) \ , \tag{5.25}$$

ya que basta con notar que $\ln n = \ln\left(\prod_{p_i|n} p_i^{\alpha_i}\right) = \sum_{p_i|n} \alpha_i \ln p_i$. Ahora bien, como $\Lambda(p_i^\beta) = \ln p_i$ para cualquier exponente β, si $p_i^{\alpha_i}$ es el factor asociado al primo p_i en la factorización de n, la contribución de los divisores de la forma p^β a (5.25) es exactamente $\alpha_i \ln p_i$. Como $\Lambda(u) = 0$ para cualquier otro divisor, se tiene la igualdad (5.25). En consecuencia, el teorema del número primo para funciones aritméticas puede reescribirse como

$$\sum_{\substack{n \le x \\ n \equiv a \pmod d}} \Lambda(n) = (1+o(1))\frac{x}{\varphi(d)} \ . \tag{5.26}$$

El siguiente teorema da un importante paso hacia adelante en la estimación de $o(1)$.

Teorema 5.2.3 (Siegel-Walfisz)**.** *En la igualdad* (5.26)*, puede tomarse*

$$o(1) = O\left(x \exp(-C_N\left(\ln x\right)^{1/2}\right)\right) = O\left(x^{1-C_N/\ln x}\right)$$

para $d \le (\log x)^N$ *y cualquier entero* N.

El teorema anterior relaciona el valor de $o(1)$ con d y x. Se sospecha además que, para cualquier $\epsilon > 0$, el Teorema 5.2.3 sigue siendo válido tomando $1 \le d \le x^{1-\epsilon}$. Sin embargo, puede ampliarse el rango $1 \le d \le (\ln x)^N$ que garantiza el teorema anterior permitiendo que la igualdad (5.26) falle en algunos números. Con esta idea en mente, se define el conjunto $\mathcal{B}$ formado por los números $0 < B < 1$ tales que existen $x_0(B), D_B > 0$, con D_B entero, de tal modo que si $x \ge x_0(B)$, $(d,a) = 1$ y $1 \le d \le \text{mín}\{x^B, y/x^{1-B}\}$, entonces

$$\pi(y;d,a) \ge \frac{\pi(y)}{2\varphi(d)}$$

cuando d no es divisible por ninguno de los elementos del conjunto $\mathcal{D}_B(x)$ (dependiente del valor x), del que se conoce que $|\mathcal{D}_B(x)| \le D_B$ y que ninguno de sus elementos es inferior a $\ln x$. Los autores de [AGP94] demostraron que $(0, 5/12) \subset \mathcal{B}$.

Escribiremos $\pi(x, y)$ para referirnos al conjunto de números primos p inferiores a x de tal manera que $p - 1$ no tiene ningún factor primo excediendo y. De igual modo que con $\mathcal{B}$, definimos el conjunto $\mathcal{E}$ formado por los números $0 < E < 1$ tales que existen números $x_2(E), \gamma(E) > 0$ cumpliendo que

$$\pi(x, x^{1-E}) \geq \gamma(E)\pi(x)$$

para todo $x \geq x_2(E)$. Se conoce que $1 - (2\sqrt{e})^{-1} \in \mathcal{E}$ [Fri89]. Con esta notación, podemos enunciar el resultado principal del artículo [AGP94].

Teorema 5.2.4. *Para todo $B \in \mathcal{B}$ y todo $E \in \mathcal{E}$ existe $x_0(B, E) > 0$ tal que $C(x) \geq x^{EB}$, siempre que $x \geq x_0$.*

Dado que $1 - (2\sqrt{e})^{-1} \in \mathcal{E}$, $(0, 5/12) \subset \mathcal{B}$, escribiendo

$$\beta = (1 - (2\sqrt{e})^{-1})\frac{5}{12} = 0{,}290306... > 0{,}2857142857142857 = 2/7 \ ,$$

podemos garantizar que $C(x) > x^{\beta-\epsilon}$ para x suficientemente grande. En particular, puede asegurarse que $C(x) > x^{2/7}$ para x suficientemente grande.

Sin embargo, no se conoce cuál es el comportamiento asintótico de $C(x)$. Una de las propuestas más referenciadas en la literatura se debe a Erdös, quien en el mismo artículo en que presentó la cota superior de la anterior sección propuso un argumento heurístico para justificar que

$$C(x) = x^{1-o(1)} \ , \tag{5.27}$$

cuando x es suficientemente grande. Sin embargo, de acuerdo con [GP02], otros autores como Dan Shanks se mostraban escépticos acerca de la validez del crecimiento asintótico predicho en (5.27). Basándose en los datos de los que disponía, Shanks sospechaba que no era posible encontrar más de $x^{1/2}$ números de Carmichael a partir de un x suficientemente grande. Como veremos en la Tabla 5.1, se tiene que $C(10^{16}) = 246683$. Por ello, la cantidad de números de Carmichael hasta $x = 10^{16}$ viene dada aproximadamente por $x^{0{,}337}$ ya que

$$\frac{\log(246683)}{\log(10^{16})} = 0{,}337008\ldots$$

lo que es indicio a favor de la visión de Shanks sobre la de Erdös.

5.3. Números de Carmichael con k factores primos

En lo siguiente, escribiremos $C_k(x)$ para referirnos a la cantidad de números de Carmichael no mayores que x y con exactamente k factores primos. Claramente, se verifica que

$$C(x) = C_3(x) + C_4(x) + C_5(x) + \ldots$$

A día de hoy, es un problema abierto determinar si, para algún entero, k la función $C_k(x)$ no está acotada. Pese a ello, es ampliamente creído que esto último es cierto. Más aún, la siguiente conjetura propuesta por Granville y Pomerance predice cuál es crecimiento asintótico para los números de Carmichael con k factores primos [GP02].

Conjetura 5.3.1. Para todo $k \geq 3$, $C_k(x) \geq x^{1/k+o(1)}$.

Si la conjetura anterior es cierta, una de sus implicaciones más inmediata es la siguiente cadena de desigualdades, ciertas para x suficientemente grande

$$C_3(x) > C_4(x) > \ldots > C_k(x) > \ldots$$

Resulta útil contrastar esta conjetura con los datos reales. Con este propósito, incluimos la Tabla 5.1, que recoge las cantidades de números de Carmichael menores o iguales que 10^m, con $3 \leq m \leq 16$, discriminando en función del número de factores primos. De acuerdo con la Conjetura 5.3.1, los números de Carmichael con 3 factores primos constituyen la clase más abundante. Ésto es indiscutiblemente cierto para $x = 10^5$, pues 12 de los 16 números de Carmichael hasta este punto tienen 3 factores primos. Sin embargo, la validez de la conjetura comienza a ser dudosa a partir de $x = 10^7$, cuando comienza a haber más números de Carmichael con 4 factores primos. Esta tendencia se mantiene en las siguientes filas de la Tabla 5.1, ya que para $x = 10^{11}$ el valor de $C_5(x)$ vuelve a sobrepasar $C_4(x)$, y de nuevo para $x = 10^{15}$ los números con 6 factores primos son los más comunes. Parece por tanto, no solo que la Conjetura 5.3.1 es falsa, sino que además el número de factores más abundante aumenta a medida que lo hace x. Sin embargo, los cálculos computacionales no son un argumento de peso suficiente para desmentir la conjetura anterior, y (a priori) nada impide la ocurrencia de un cambio de tendencia para valores de x mayores que $x = 10^{16}$.

x	$C_3(x)$	$C_4(x)$	$C_5(x)$	$C_6(x)$	$C_7(x)$	$C_8(x)$	$C_9(x)$	$C_{10}(x)$	$C(x)$
10^3	1								1
10^4	7								7
10^5	12	4							16
10^6	23	19	1						43
10^7	47	55	3						105
10^8	84	144	27						225
10^9	172	314	146	14					646
10^{10}	335	619	492	99	2				1547
10^{11}	590	1179	1336	459	41				3605
10^{12}	1000	2102	3156	1714	262	7			8241
10^{13}	1858	3639	7082	5270	1340	89	1		19279
10^{14}	3284	6042	14938	14401	5359	655	27		44706
10^{15}	6083	9938	29282	36907	19210	3622	170		105212
10^{16}	10816	16202	55012	86696	60150	16348	1436	23	246683

Tabla 5.1: Valores de $C_k(x)$ y $C(x)$ cuando $k = 3, 4, \ldots, 10$ y se toma $x = 10^m$, con $m = 3, 4, \ldots, 16$.

Por otra parte, sí se conoce una cota superior para $C_3(x)$ que parece respaldar la validez de la Conjetura 5.3.1. Ésta se resume en el siguiente resultado, tomado de [BN97].

Teorema 5.3.2. *$C_3(x) = O(x^{5/14+o(1)})$ para x suficientemente grande.*

Es claro que $x^{1/3+o(1)} = O(x^{5/14} + o(1))$, de modo que el teorema anterior no contradice la Conjetura 5.3.1. Más aún, comparando $5/14 = 0{,}35714\ldots \sim 1/3$ vemos que el crecimiento asintótico conjeturado es de un orden muy similar a la cota del teorema, lo que sugiere que quizás esta última no pueda reducirse mucho más.

Como hemos comentado en la página anterior, aún no se conoce con seguridad si alguna de las funciones $C_k(x)$ crece indefinidamente a medida que lo hace x. Sin embargo,

un resultado publicado en 2016 por Thomas Wright ha abierto un nuevo camino para ahondar en esta cuestión. El siguiente teorema, tomado de [Wri12] (comprobar referencia), relaciona el teorema de Maynard-Tao (Teorema 4.1.6, Sección 4) con el crecimiento de las funciones $C_k(x)$.

Teorema 5.3.3. *Si la cota $r > D\exp(8m)$ del Teorema 4.1.6 se reemplaza por una cota polinomial de la forma $r > m^T$ para algún $T > 0$, entonces para infinitos valores de k es cierto que $C_k(x) \to \infty$ cuando $x \to \infty$.*

Este último teorema pone (de nuevo) de manifiesto la relevancia del teorema de Maynard-Tao en teoría de números. Solo dentro de los resultados incluídos en este trabajo hemos visto que está relacionado con la posibilidad de generar infinitos números de Carmichael utilizando formas universales (Sección y con el crecimiento de las funciones $C_k(x)$. Por sus aplicaciones y su valor en sí mismo, el teorema de Maynard-Tao es uno de los resultados más importante en teoría de números de los últimos años.

Capítulo 6

Conclusiones

Al término de este trabajo, la siguiente pregunta es necesaria: ¿cuál es la utilidad de los resultados que se han demostrado? Más concretamente, ¿por qué merece la pena seguir estudiando los números de Carimchael? En primer lugar, los números de Carmichael nos recuerdan que se ha de ser cauto a la hora de analizar el recíproco de un teorema. Por otra parte, el conocimiento de la distribución de los números de Carmichael permite acotar inferiormente la cantidad de pseudoprimos de Fermat para una cierta base. Sin embargo, a día de hoy se emplean tests de primalidad más modernos que el pequeño teorema. El más común es el test de Rabin-Miller, que se basa en comprobar si un entero es o no un pseudoprimo fuerte. Sin embargo, puede demostrarse [Rab80] que no existen enteros pseudoprimos fuertes para todas sus bases, i.e. no existen números de Carmichael "fuertes". Por lo tanto, su aplicación para la detección de falsos números primos parece hacer aguas. Pese a ello, el camino que hemos seguido para introducir la noción de número de Carmichael pasaba por la demostración del Teorema 2.2.20, que resulta verdaderamente útil en el estudio de pseudoprimos.

Como señalabamos en la Introducción, el verdadero valor del estudio de los números de Carmichael reside en el conocimiento matemático que surge de la búsqueda de respuestas para preguntas que se plantean en términos de estos números. Resulta sorprendente leer las herramientas que se desarrollaron para la demostración del Teorema 5.2.4, y aunque el objetivo de su nacimiento fuera la demostración de la existencia de infinitos números de Carmichael, desde luego son susceptibles de aplicarse en otros contextos. Adicionalmente, en la prueba del Lema 5.1.4 acudimos a diversos resultados relacionados con una función importante en teoría de números, la distribución de los números primos y la suma de funciones aritméticas. Por esto, uno de los objetivos de este texto es el de explorar otras herramientas de teoría de números más allá de los números de Carmichael. Igualmente, este trabajo busca definir de forma clara la relación existente entre los números de Carmichael y algunos de los problemas abiertos en teoría de números. Este último hecho queda bien reflejado en los métodos de construcción a través de formas universales, estudiados en el Capítulo 4. Al fin y al cabo, gracias al criterio de Korselt todos los métodos se reducen a la búsqueda de números primos en progresiones aritméticas, i.e. en determinar los enteros n para los que una familia $\{g_i n + h_i\}_{i=1}^{k}$ está compuesta enteramente por números primos. Así, el problema de generar números de Carmichael deriva a un problema mucho más general en teoría de números, y el estudio de los números de Carmichael desemboca en nuevas líneas de investigación relacionadas con primalidad. Este hecho enfatiza la idea de que el estudio de los números de Carmichael motiva el progreso matemático.

Otra conclusión importante que debe extraerse de la lectura de este trabajo es el desconocimiento que, incluso a día de hoy, envuelve a los números de Carmichael. Como exponíamos en la introducción del Capítulo 5, no se conoce algo tan elemental como cuál es el comportamiento asintótico de la función C. Sin lugar a duda, esto es debido a la dificultad intrínseca a su estudio. Hemos podido comprobar que la prueba de la cota superior es la parte más técnica y compleja de este trabajo, y aún así se trata de un resultado sin una aplicación destacable. Además, la complejidad de esta última no es comparable a la demostración del Teorema 5.2.4, que de nuevo no deja de ser una cota inferior para la función C.

En definitiva, el estudio de los números de Carmichael estimula el contacto con diferentes campos, y es un tema adecuado para introducirse en otras áreas más especializadas que en la actualidad reciben gran antención por parte de los investigadores. Dos de las aptitudes más importantes a la hora de realizar trabajo matemático son un amplio conocimiento en diversos temas y la capacidad de combinar con coherencia este conocimiento, y sin lugar a duda el estudio de los números de Carmichael ejercita ambas.

Bibliografía

[AGP94] W. R. Alford, A. Granville, y C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Mathematics*, 139(3):703–722, 1994.

[Bee50] N. G. W. H. Beeger. On composite numbers n for which $a^{n-1} \equiv 1$ (mód n) for every a prime to n. *Scripta math*, 16(1):133–135, 1950.

[BN97] R. Balasubramanian y S. V. Nagaraj. Density of Carmichael numbers with three prime factors. *Mathematics of computation*, 66(220):1705–1708, 1997.

[BW80] R. Baillie y S. S. Wagstaff. Lucas pseudoprimes. *Mathematics of Computation*, 35(152):1391–1417, 1980.

[Car10] R. D. Carmichael. Note on a new number theory function. *Bulletin of the American Mathematical Society*, 16(5):232–238, 1910.

[Car12] R. D. Carmichael. On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1$ (mód p). *The American Mathematical Monthly*, 19(2):22–27, 1912.

[Che39] J. Chernick. On Fermat's simple theorem. *Bulletin of the American Mathematical Society*, 45(4):269–274, 1939.

[Cip04] M. Cipolla. Sui numeri composti p, che verificano la congruenza di Fermat $a^{p-1} \equiv 1$ (mód p). *Annali di Matematica Pura ed Applicata*, 9(1):139–160, 1904.

[Dab89] H. Daboussi. On the prime number theorem for arithmetic progressions. *Journal of Number Theory*, 31(3):243–254, 1989.

[dB51] N. G. de Bruijn. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A: Mathematical Sciences*, 54(1):50–60, 1951.

[Dic04] L. E. Dickson. A new extension of Dirichlet's theorem on prime numbers. *Messenger of Math*, 33(1):155–161, 1904.

[Dup52] H. J. A. Duparc. On Carmichael numbers. *Simon Stevin*, 29(1):21–24, 1952.

[Erd56] P. Erdös. On pseudoprimes and Carmichael numbers. *Publicationes Mathematicae Debrecen*, 4(1):201–206, 1956.

[Eü41] L. Eüler. Theorematum quorundam ad numeros primos spectantium demonstratio. *Commentarii academiae scientiarum Petropolitanae*, pages 141–146, 1741.

[Fle91] C. R. Fletcher. A reconstruction of the Frénicle-Fermat correspondence of 1640. *Historia Mathematica*, 18(4):344–351, 1991.

[Fri89] J. B. Friedlander. Shifted primes without large prime factors. *Number theory and applications*, pages 393–401, 1989.

[GHDH79] F. W. Gehring, P. R. Halmos, C. DePrima, y I. Herstein. *Undergraduate Texts in Mathematics*. Springer, 1979.

[GP02] A. Granville y C. Pomerance. Two contradictory conjectures concerning Carmichael numbers. *Mathematics of Computation*, 71(238):883–908, 2002.

[HW79] G. H. Hardy y E. M. Wright. *An introduction to the theory of numbers*. Oxford university press, 1979.

[KLS13] M. Krizek, F. Luca, y L. Somer. *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. Springer Science & Business Media, 2013.

[Knö53] W. Knödel. Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x. *Archiv der Mathematik*, 4(4):282–284, 1953.

[Kor99] A. Korselt. Probleme chinois. *L'intermédiaire math*, 6(1):143–143, 1899.

[NZM13] I. Niven, H. S. Zuckerman, y H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 2013.

[Pou38] P. Poulet. *Table des nombres composes verifiant le theoreme de Fermat pour le module 2 jusqu'a 100.000. 000*. 1938.

[PSW80] C. Pomerance, J. L. Selfridge, y S. S. Wagstaff. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151):1003–1026, 1980.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primality. *Journal of number theory*, 12(1):128–138, 1980.

[Rib12] P. Ribenboim. *The new book of prime number records*. Springer Science & Business Media, 2012.

[Ros39] B. Rosser. The n-th prime is greater than $n \log n$. *Proceedings of the London Mathematical Society*, 2(1):21–44, 1939.

[WH82] D. Woods y J. Huenemann. Larger Carmichael numbers. *Computers & Mathematics with Applications*, 8(3):215–216, 1982.

[Wil95] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141(3):443–551, 1995.

[Wri12] T. Wright. The impossibility of certain types of Carmichael numbers. *Integers*, 12(5):951–964, 2012.

[Yor78a] M. Yorinaga. Numerical computation of Carmichael numbers. *Mathematical Journal of Okayama University*, 20(1), 1978.

[Yor78b] M. Yorinaga. Numerical computation of Carmichael numbers. *Mathematical Journal of Okayama University*, 20(2), 1978.